

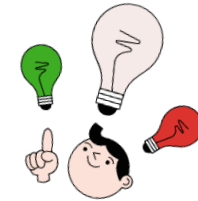
GDPR

Le soluzioni tecnologiche a supporto dell'azienda e del DPO



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



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.

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**

GDPR compliant ?



Written by Daniel J. Solove

www.teachprivacy.com

Illustrated by Ryan Beckwith

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.

II 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.



I 7 principi del regolamento

Liceità e
correttezza

Trasparenza

Limitazioni
delle finalità dei
trattamenti

Minimizzazione

Esattezza

Limitazione
della
conservazione

Integrità e
riservatezza

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.

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)

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 ?



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

Recenti provvedimenti del Garante



Provvedimento dell'11 dicembre 2019 [9244358]



Provvedimento dell'11 dicembre 2019 [9244365]

Provvedimento dell'11 dicembre 2019

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della prof.ssa Licia Califano, componente, della dott.ssa Giovanna Bianchi Clenici, componente e del dott. Giuseppe Busia, segretario generale;

VISTA la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 concernente la protezione dei dati personali, e in particolare l'articolo 17 della stessa direttiva;

VISTO il Regolamento generale sulla protezione dei dati (Regolamento (UE) 2016/679) del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito "Regolamento (UE) 2016/679");

VISTO il Codice in materia di protezione dei dati personali (Decreto del Presidente della Repubblica n. 30 del 6 giugno 2003, n. 196, come modificato dal D.Lgs. n. 101 del 10 agosto 2018, n. 101, di seguito "Codice");

VISTI gli atti d'ufficio e le osservazioni formulate dal settore generale a sensi dell'art. 17 del regolamento (UE) 2016/679;

RELATORE la dott.ssa Augusta Iannini;

Sanzioni GDPR Italia 2019: ENI Gas e Luce SpA deve pagare 11.500.000 Euro per 2 ordinanze del Garante Privacy

VEDI ANCHE Comunicato stampa del 17 gennaio 2020
VEDI ANCHE Comunicato stampa del 17 gennaio 2020

[Doc. web n. 9244365]

Registro dei provvedimenti n. 22 del 11 dicembre 2019

1. I RECLAMI PENDENTI

Sono pervenuti a questa Autorità diversi reclami aventi ad oggetto il trattamento dei dati personali di clienti (anche potenziali) posti in essere da Eni gas e luce S.p.A. (di seguito "Eni") nell'ambito della fornitura di energia elettrica e gas, mediante la conclusione di contratti non richiesti nel mercato libero. In particolare, i reclamanti hanno lamentato di aver preso conoscenza della stipula del contratto solo a seguito di ricezione di lettera di chiusura pervenuta da parte del presidente fondatore o di recapito della prima

Il richiedente ha portato avanti un'attenta attività di monitoraggio della modulistica diligente e all'esito di tale attività ha individuato alcune irregolarità. In particolare, il richiedente ha segnalato che la Società nei giorni 18, 19 e 20 febbraio 2019 ha inviato ai clienti una modulistica contenente informazioni e dati personali non pertinenti e non autorizzati. Inoltre, il richiedente ha segnalato che la Società ha fornito informazioni e dati personali non pertinenti e non autorizzati ai propri dipendenti e a terzi. Il richiedente ha chiesto che la Società sia sanzionata e che i dati personali non pertinenti e non autorizzati siano cancellati.



Ordinanza ingiunzione nei confronti di Vincall s.r.l.s - 11 aprile 2019 [9116053]

VEDI ANCHE Comunicato stampa del 17 gennaio 2020

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clenici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO l'art. 1, comma 2, della legge 24 novembre 1983 n. 480, in vigore dal 1° gennaio 1984, concernente la disciplina dell'attività di vigilanza e di controllo del Garante per la protezione dei dati personali;

VISTO l'art. 1, comma 2, della legge 24 novembre 1983 n. 480, in vigore dal 1° gennaio 1984, concernente la disciplina dell'attività di vigilanza e di controllo del Garante per la protezione dei dati personali;

RELATORE la dott.ssa Augusta Iannini;



Marketing: dal Garante privacy sanzione di 27 milioni e 800 mila euro a Tim

Marketing: dal Garante privacy sanzione di 27 milioni e 800 mila euro a Tim

Il Garante per la privacy ha irrogato a Tim spa una sanzione di 27.802.946 euro per numerosi trattamenti illeciti di dati legati all'attività di marketing. Le violazioni hanno interessato nel complesso alcuni milioni di persone.

Dal gennaio 2017 ai primi mesi del 2019, sono pervenute all'Autorità centinaia di segnalazioni relative, in particolare, alla ricezione di chiamate promozionali indesiderate effettuate senza consenso o nonostante l'iscrizione delle utenze telefoniche nel Registro pubblico delle opposizioni, oppure ancora malgrado il fatto che le persone contattate avessero espresso alla società la volontà di non ricevere telefonate promozionali. Irregolarità nel trattamento dei dati venivano lamentate anche nell'ambito dell'offerta di concorsi a premi e nella modulistica sottoposta agli utenti da Tim.

Dalla complessa attività istruttoria che ne è derivata, svolta anche con il contributo del Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza, sono emerse numerose e gravi violazioni della disciplina in materia di protezione dei dati personali.

Tim ha dimostrato di non avere sufficiente coerenza di fondamentali aspetti dei trattamenti di dati effettuati (accountability).

Tra i milioni di telefonate promozionali effettuate in sei mesi nei confronti di "non clienti" l'Autorità ha accertato che le società di call center incaricate da Tim hanno, in molti casi, contattato gli interessati senza il loro consenso. Una persona è stata chiamata 155 volte in un mese. In circa duecentomila casi, sono state contattate anche numerazioni "fuori lista", cioè non presenti negli elenchi delle persone contattabili di Tim. Sono state rilevate poi altre condotte illecite come l'assenza di controllo da parte della società sull'operato di alcuni call center; l'errata gestione e il mancato aggiornamento delle black list dove vengono registrate le persone che non vogliono ricevere pubblicità; l'acquisizione obbligata del consenso a fini promozionali per poter aderire al programma "Tim Party" con i suoi sconti e premi.

Nella gestione di alcune app destinate alla clientela, inoltre, sono state fornite informazioni non corrette e non trasparenti sul trattamento dei dati e sono state adottate modalità di acquisizione del consenso non valide. In alcuni casi è stata utilizzata modulistica cartacea con richiesta di un unico consenso per diverse finalità, inclusa quella di marketing.

La gestione dei data breach non è poi risultata efficiente, così come inadeguate sono risultate l'implementazione e la gestione da parte della Società dei sistemi che trattano dati personali (con violazione del principio di privacy by design). Disallineamenti sono emersi tra le black list di Tim e quelle dei call center incaricati, così come per le registrazioni audio dei contratti stipulati telefonicamente (verbal order). Le utenze di clienti di altri operatori, detenute da Tim in quanto gestore delle Reti, sono state conservate per un tempo superiore ai limiti di legge e inserite, senza il consenso degli interessati, in alcune campagne promozionali.

Oltre alla sanzione, l'Autorità ha imposto a Tim 20 misure correttive, tra divieti e prescrizioni. In particolare, ha vietato a Tim l'uso dei dati a fini di marketing di chi aveva espresso ai call center il proprio diniego a ricevere telefonate promozionali, dei soggetti presenti in black list e dei "non clienti" che non avevano dato il consenso.

La società non potrà più utilizzare neanche i dati della clientela raccolti mediante le app "My Tim", "Tim Personal" e "Tim Smart Kid"

di euro 1.500.000 (un milione cinquecentomilaquarantasei);

VISTA la documentazione in atti;

VISTA la legge n. 30/1981, e le successive modificazioni e integrazioni;

VISTE le osservazioni formulate dal segretario generale e dalla commissione di delibere del 25 giugno 2020;

RELATORE la dott.ssa Augusta Iannini;



Multa di 2.018.000 € a Vincall Srls per gestione contatti senza consenso



IL PRESIDENTE
Soro
IL RELATORE
Iannini
IL SEGRETARIO GENERALE
Busia



Ordinanza ingiunzione nei confronti di R.T.I. - Reti Televisive Italiane s.p.a. - 6 febbraio 2020 [9283121]

[Doc. web n. 9283121]

Ordinanza ingiunzione nei confronti di R.T.I. - Reti Televisive Italiane s.p.a. - 6 febbraio 2020

Registro dei provvedimenti n. 28 del 6 febbraio 2020

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della prof.ssa Licia Califano e della dott.ssa Giovanna Bianchi Clenici, componenti e del dott. Giuseppe Busia, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito, "Regolamento");

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

VISTO il reclamo presentato al Garante in data 30 ottobre 2018, ai sensi dell'art. 77 del Regolamento, con il quale la sig.ra XX, rappresentata e difesa dall'Avv. XX ha lamentato una violazione della disciplina in materia di protezione dei dati personali in relazione alla trasmissione, durante la puntata de "Le Iene" del XX 2018, di un servizio dal titolo "XX" nel quale la reclamante sarebbe stata resa identificabile attraverso l'utilizzo della sua voce e di altre informazioni relative alla sua sfera personale;

CONSIDERATO che l'interessata ha, in particolare, rappresentato che:

nel servizio viene intervistata una donna dal volto oscurato, presumibilmente un'attrice, alla quale viene associata la propria voce e informazioni personali che lei aveva confidato ad un cliente;

- l'insieme delle informazioni trattate nell'intervista (la città di origine, il fatto di aver cambiato da poco casa e di avere dei figli, la precedente professione svolta, il luogo e il periodo di una vacanza che avrebbe intrapreso di lì a breve, di aver portato poco prima i figli a sciare, specificando la regione, e l'abitudine di andare ogni anno in vacanza in un posto, anch'esso specificato) unitamente alla sottrazione fraudolenta della voce hanno consentito a molti di riconoscerla;

- la divulgazione non autorizzata dei suoi dati personali è avvenuta «con un evidente artificio/raggio» da un soggetto, non presentatosi come giornalista o inviato de Le Iene, XX;

- la sua richiesta di rimozione del video, accessibile anche in rete, rivolta a Mediaset S.p.a. è rimasta priva di riscontro e pertanto chiede al Garante, ai sensi dell'art. 17 del Regolamento, di ordinare alla predetta Società di cancellare il servizio in questione e di disporre nei confronti di quest'ultima una sanzione;

VISTA la nota di RTI- Reti Televisive Italiane s.p.a. del 4 febbraio 2019 nella quale precisa che:

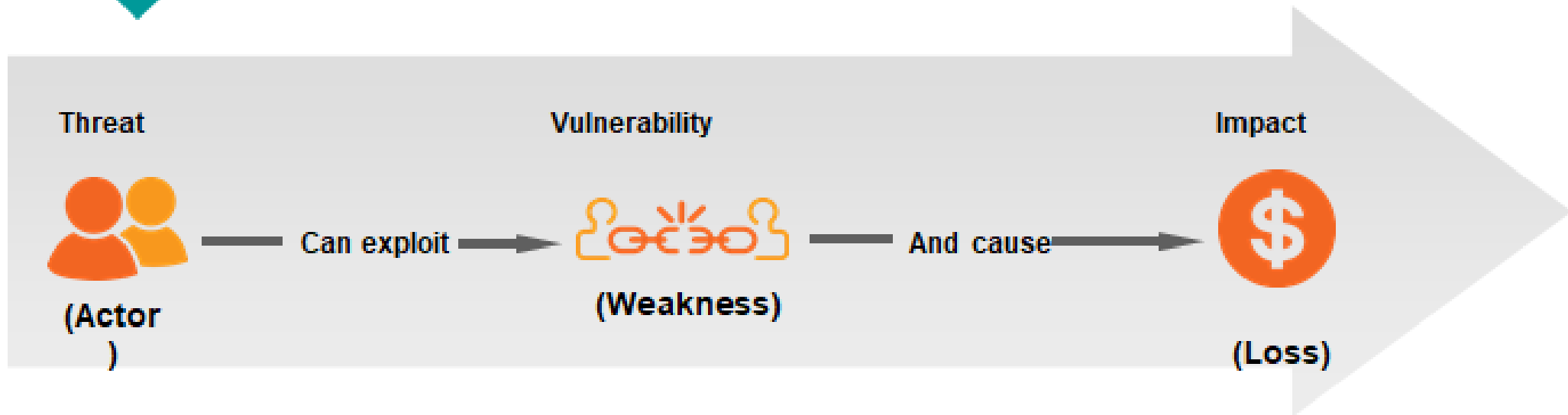
- il mancato riscontro alla missiva del legale della reclamante è risultata imputabile esclusivamente a un difetto di conoscenza, derivato probabilmente da un vizio originario, ovvero dal suo inoltrare non alla società scrivente, bensì alla sede della società

Articolo 32 – Sicurezza del trattamento

- 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:
 - la pseudonimizzazione e la cifratura dei dati personali;*
 - la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
 - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*
 - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.**
- 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.*
- 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.*
- 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.*

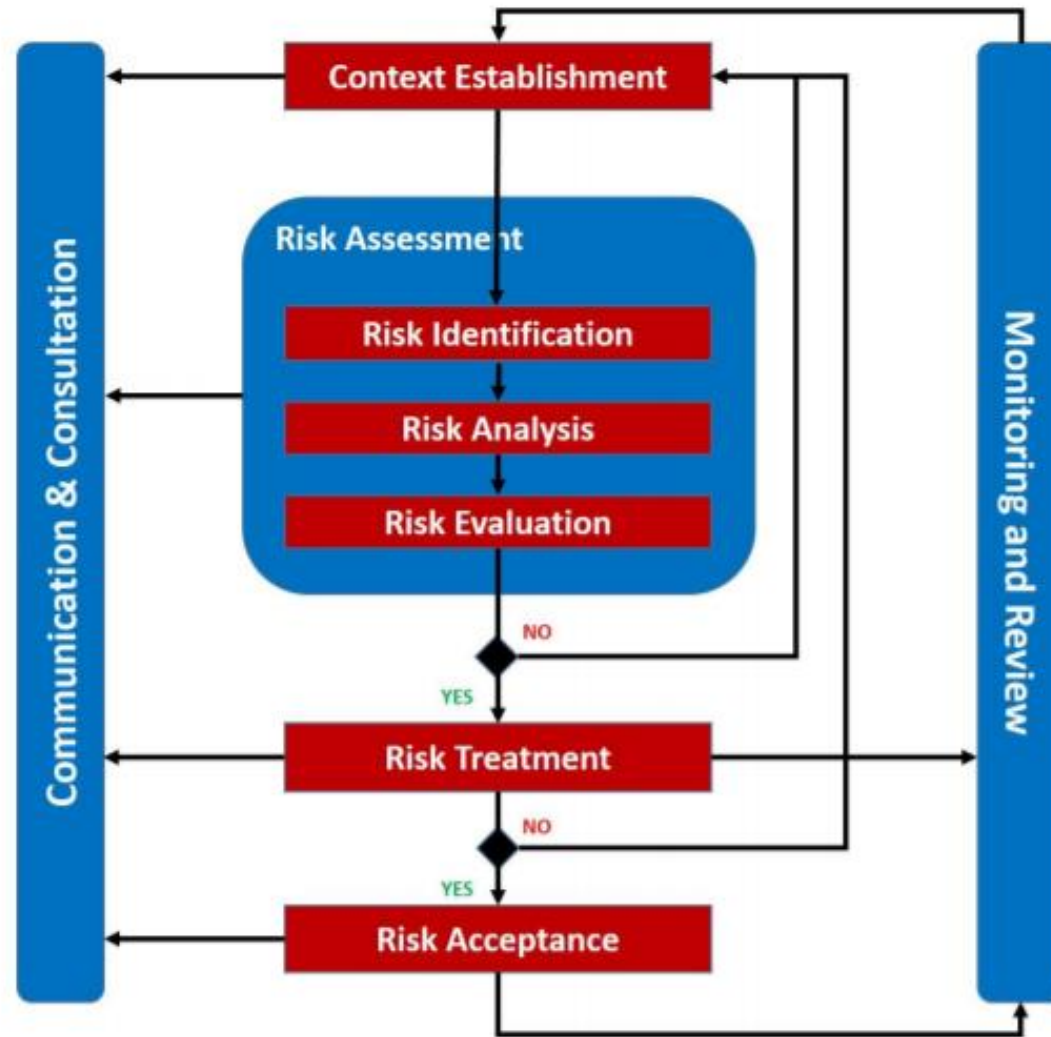
Risk Management Approach

Security risk exists when ...



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.

Risk Management Approach



ENISA Methodology for GDPR IT Risk Management

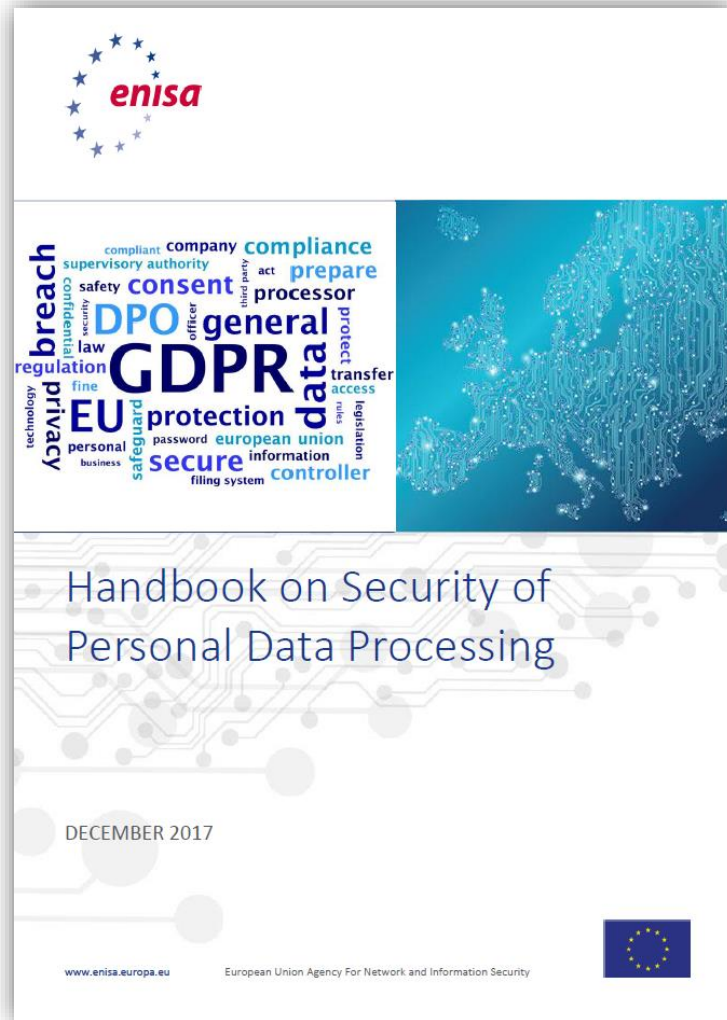


Table of Contents

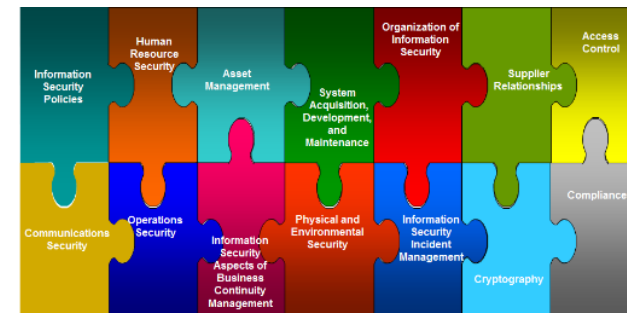
Executive Summary	6
1. Introduction	8
1.1 Background	8
1.2 Scope and Objectives	9
1.3 Methodology	9
1.4 Structure	9
2. Risk assessment and security measures for personal data	10
2.1 Methodological steps overview	10
2.1.1 Step 1: Definition of the processing operation and its context	10
2.1.2 Step 2: Understanding and evaluating impact	10
2.1.3 Step 3: Definition of possible threats and evaluation of their likelihood	12
2.1.4 Step 4: Evaluation of risk	15
2.1.5 Step 5: Security measures	16
2.2 Use cases and approach of the report	16
8. Conclusions	52
Annex A: Organizational and Technical Measures	55
A.1 Proposed Measures for Low Risk Level	55
A.2 Proposed Measures for Medium Risk Level	60
A.3 Proposed Measures for High Risk Level	64

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
1.1.	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.	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Very high
1.2.	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.	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Very high
1.3.	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.	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Very high

P	ASSESSMENT AREA	PROBABILITY	
		LEVEL	SCORE
	NETWORK AND TECHNICAL RESOURCES	<input type="checkbox"/> Low	1
		<input type="checkbox"/> Medium	2
		<input type="checkbox"/> High	3
	PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	<input type="checkbox"/> Low	1
		<input type="checkbox"/> Medium	2
		<input type="checkbox"/> High	3
	PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	<input type="checkbox"/> Low	1
		<input type="checkbox"/> Medium	2
		<input type="checkbox"/> High	3
	BUSINESS SECTOR AND SCALE OF PROCESSING	<input type="checkbox"/> Low	1
		<input type="checkbox"/> Medium	2
		<input type="checkbox"/> High	3

R

THREAT OCCURRENCE
PROBABILITY

IMPACT LEVEL

	Low	Medium	High / Very High
Low	Low Risk	Medium Risk	High Risk
Medium	Low Risk	Medium Risk	High Risk
High	Medium Risk	High Risk	High Risk

Legend



Low Risk



Medium Risk



High Risk

Impact evaluation (Esempio)

La proposta è, sulla base delle principali best practices 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

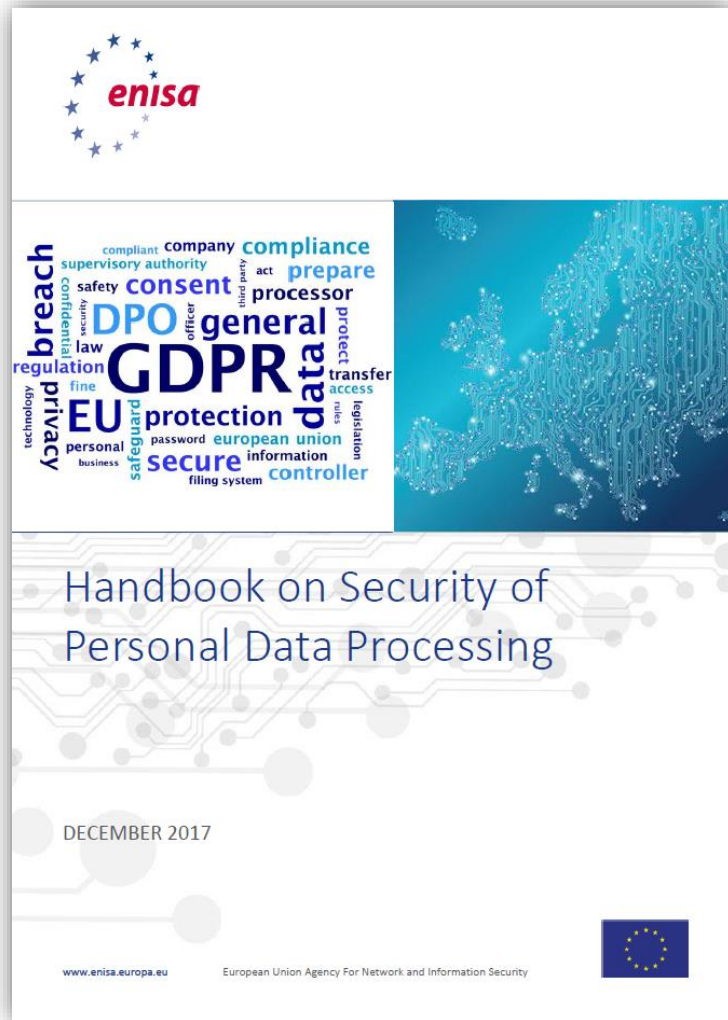


Impatti	da	a
Basso	1	4
Medio	5	7
Alto	8	9

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



Handbook on Security of Personal Data Processing
December 2017

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	Low Risk	Medium Risk	High Risk
	Medium	Low Risk	Medium Risk	High Risk
	High	Medium Risk	High Risk	High Risk

Legend

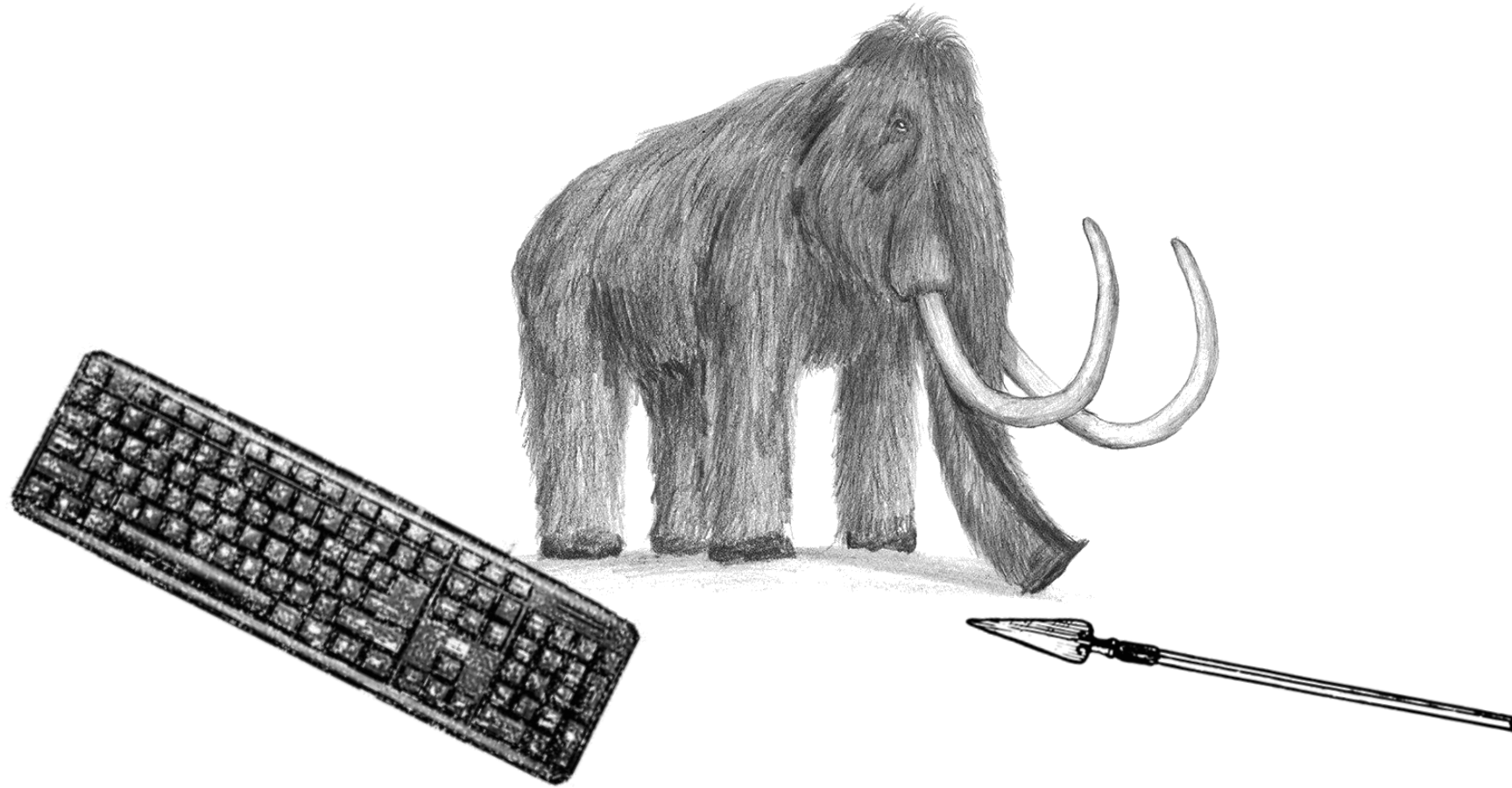
Low Risk
 Medium Risk
 High Risk

Table 6: Evaluation of risk

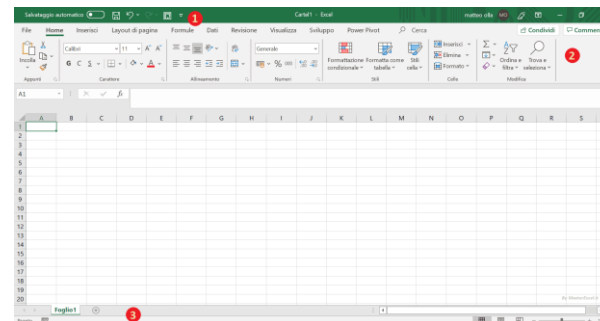
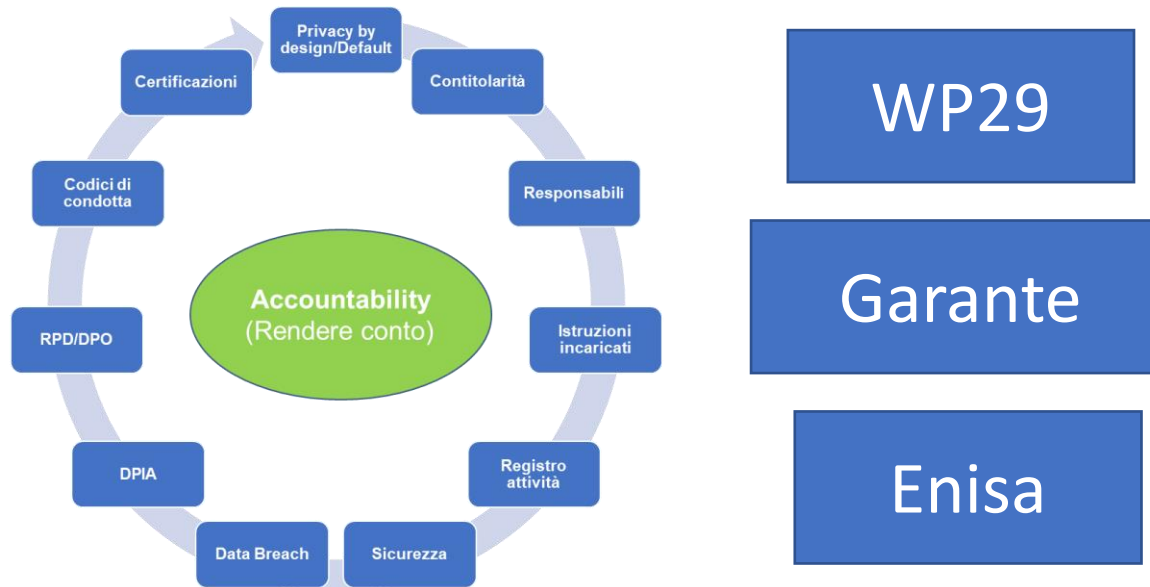


Annex A: Organizational and Technical Measures	55
A.1 Proposed Measures for Low Risk Level	55
A.2 Proposed Measures for Medium Risk Level	60
A.3 Proposed Measures for High Risk Level	64

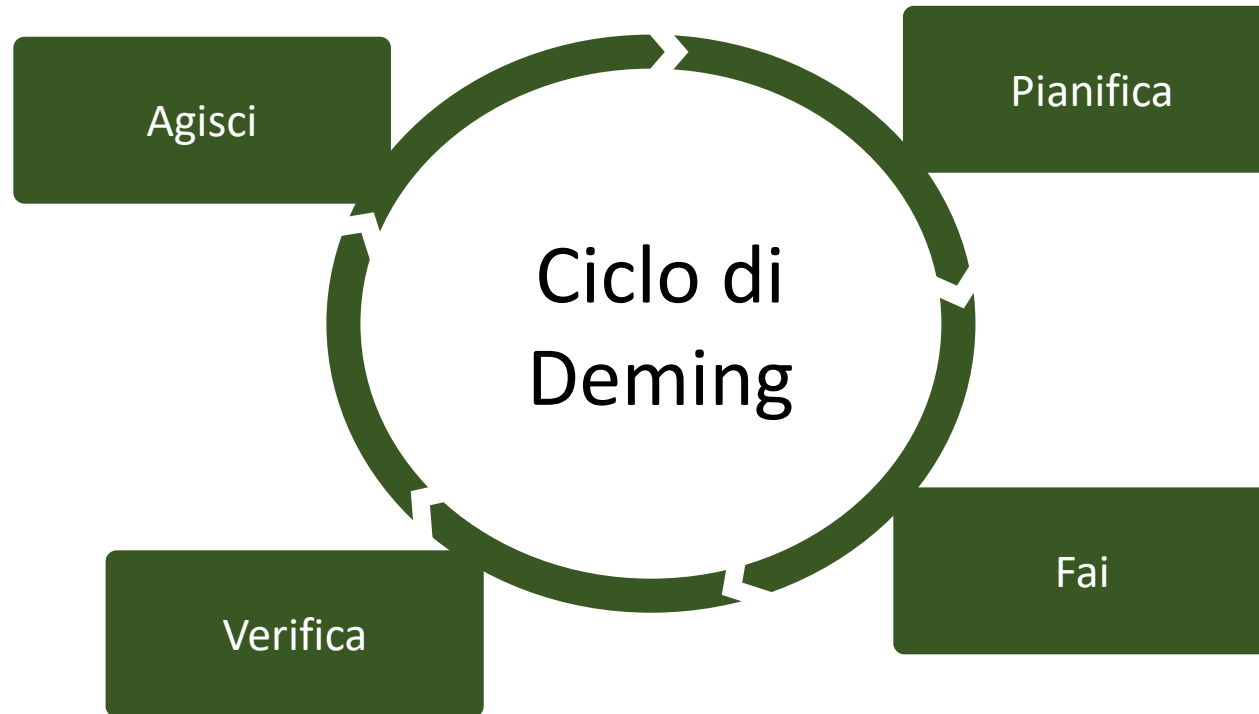
Realizzare strumenti informatici



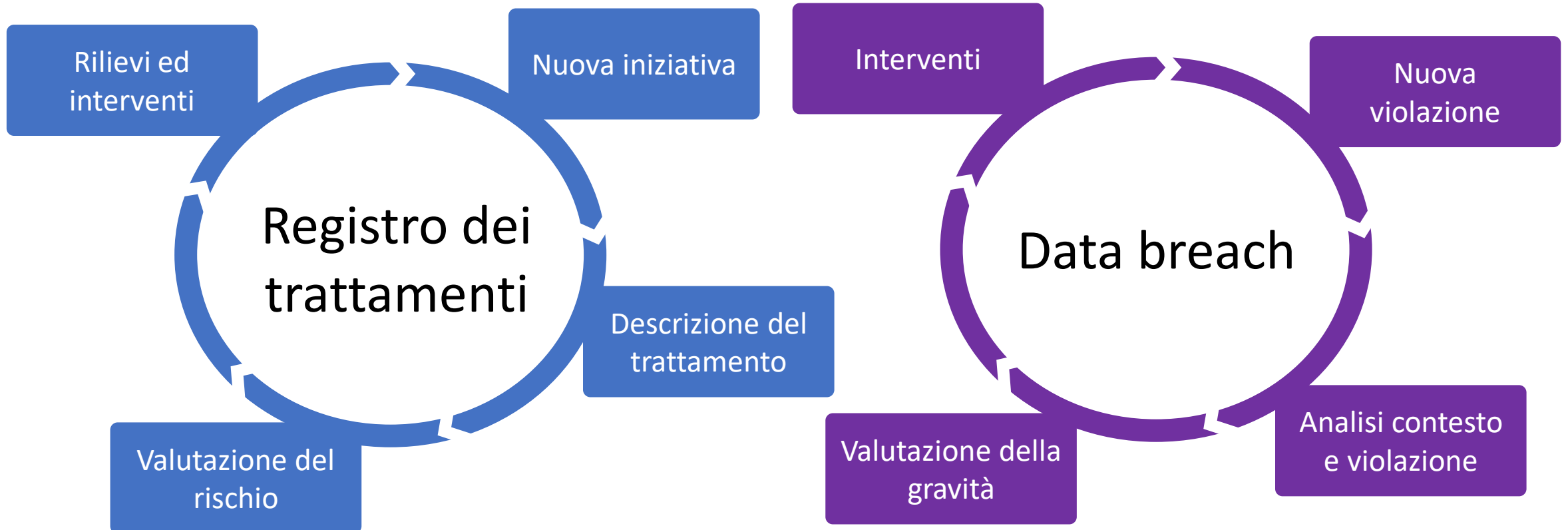
«Strumenti base» per la privacy



Comprendere (creare) i processi privacy



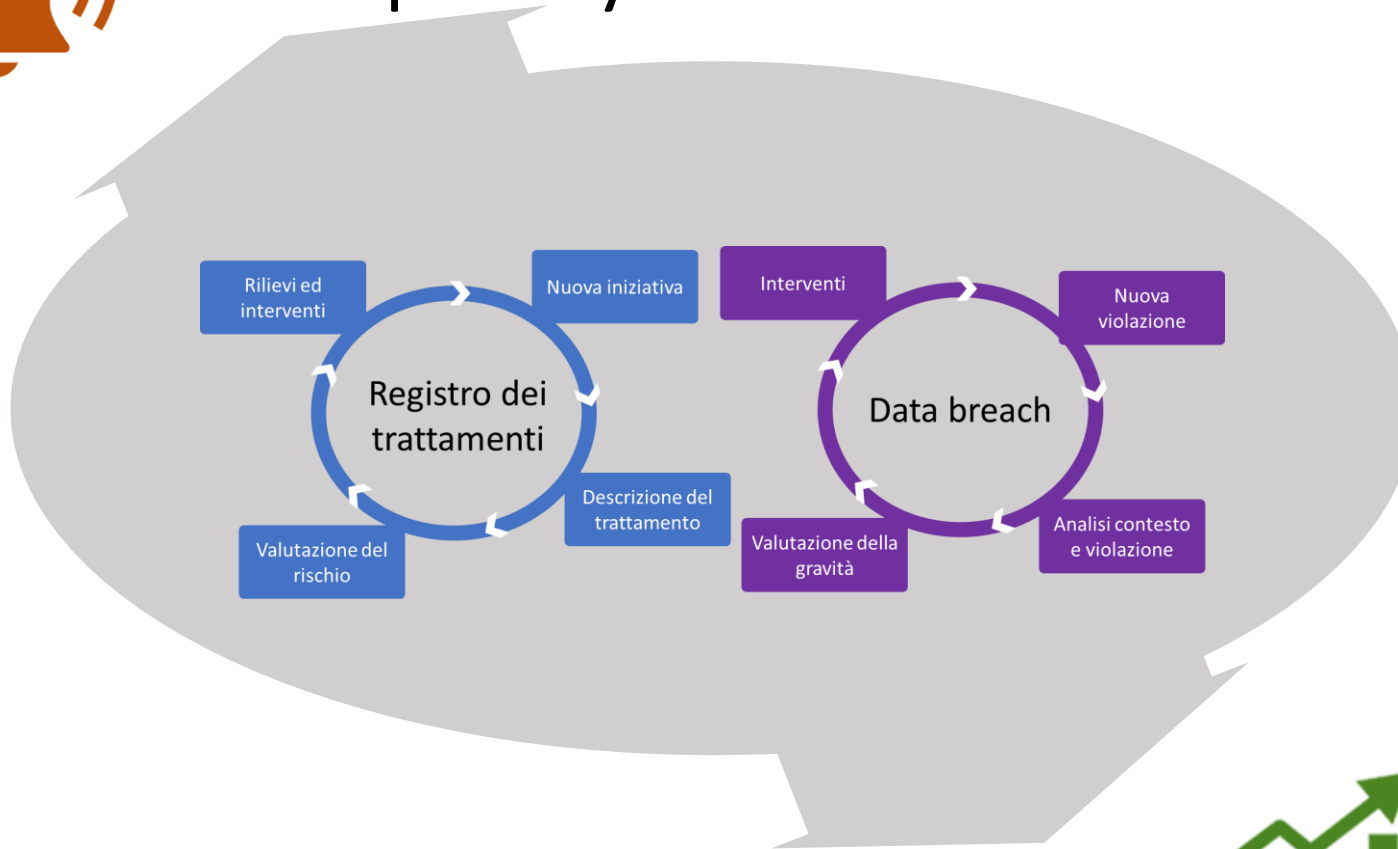
Comprendere (creare) i processi privacy



Comprendere (creare) i processi privacy



Ufficio privacy



Governance integrata in azienda

Compliance

Valutazione del rischio

Processi privacy

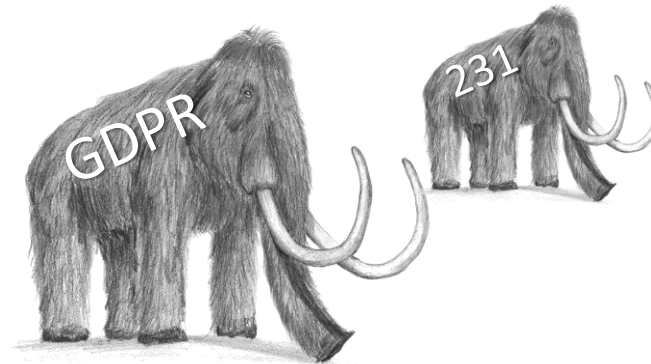


Organizzazione

Catalogo asset

Organigramma

Governance integrata in azienda



Compliance

Processi privacy

Rischio
Cyber ed IT

Organizzazione

Registro dei
trattamenti

Data breach

Catalogo
asset

Organigramma

(Nessun animale è stato maltrattato durante questo webinar)

