Regolamento generale sulla protezione dei dati personali

(General Data Protection Regulation – GDPR)

Approccio e soluzioni IBM al GDPR

NOTICE:

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsibility for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Agenda

- GDPR: overview obblighi e requisiti
- Cosa si deve fare per indirizzare la conformità al GDPR
- Approccio e soluzioni IBM
- Why IBM

La General Data Protection Regulation (GDPR)

- La General Data Protection Regulation (GDPR) è stata pubblicata Il 4 maggio 2016, ed entrerà in vigore, dopo un periodo di transizione di due anni, il 25 maggio 2018 per ogni organizzazione che opera nel mercato EU
- Diversamente dalla precedente Data Protection Directive del 1995, la GDPR cerca di creare un framework legislativo unificato e armonizzato per tutte le nazioni EU
- La non-compliance può portare a sanzioni elevate, fino a € 20ml o al 4% del fatturato annuale complessivo; è quindi indispensabile, sulla base di questi elementi, essere in grado di conoscere, governare e proteggere i dati personali.

Novità introdotte

- Il Regolamento 2016/679 sulla General Data Protection Regulation (GDPR), indica le linee da seguire sulla gestione e la protezione dei Dati.
- Il GDPR si basa sulla normativa di protezione dei dati attualmente in vigore negli Stati membri dell'UE, modifica alcune regole esistenti e aggiunge un numero significativo di nuovi obblighi per le organizzazioni, così come nuovi diritti per gli individui. Espande anche l'ambito territoriale della sua applicazione alle organizzazioni che risiedono al di fuori dell'UE, così come il campo di applicazione dai soli titolari del trattamento, ai data controller e data processors.
- Il termine per l'adeguamento è Maggio 2018 e i concetti chiave e dettagli delle principali novità introdotte sono:

  - ✓ Sanzioni in caso di data breach o inadempienze normative.
  - ✓ Se l'azienda non ha sede in Europa, sarà comunque necessario rispettare il regolamento.
  - ✓ La definizione di dati personali è più ampia, portando un maggior numero di dati nel perimetro regolamentato.
  - ✓ Il consenso dei genitori per i dati dei bambini.
  - ✓ Le modifiche alle regole per ottenere un valido consenso.
  - ✓ Per alcune società la nomina di un responsabile della protezione dei dati (DPO) sarà obbligatoria.
  - ✓ L'obbligatorietà dell'introduzione di valutazioni di impatto del rischio sulla privacy.
  - ✓ Nuovi obblighi di notifica in caso di violazione.
  - ✓ Il diritto all'oblio.
  - ✓ Il trasferimento internazionale dei dati.
  - ✓ Responsabilità del trattamento dei dati.
  - ✓ Portabilità dei dati.
  - ✓ Privacy by design.

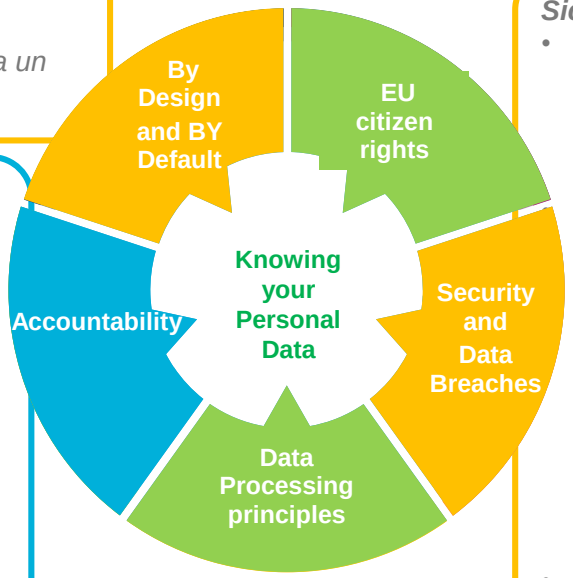
Normative GDPR: doveri e obblighi fondamentali

Data protection By Design and By Default Art 25

- *«..**misure tecniche e organizzative adeguate**, ..., volte ad attuare in modo efficace i principi di protezione dei dati, ..., e a integrare nel trattamento le necessarie garanzie»* per la conformità alla normativa e la tutela dei diritti dell'interessato
- *«... che siano trattati, per impostazione predefinita, **solo i dati personali necessari** ... Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità»*
- *«.. **non siano resi accessibili dati personali** a un numero indefinito di persone fisiche ..»*

***Diritti dei cittadini europei** Art. 12 to 20 e altri*

- Trasparenza
- Diritto all'accesso, rettifica e cancellazione (diritto "all'oblio")
- Diritto di limitazione al trattamento
- Diritto alla portabilità dei dati
- Diritto di opposizione e processo decisionale automatizzato
- Diritto di reclamo e ricorso (Art. 77-79)
- Diritto al risarcimento (Art. 82)



***Sicurezza dei dati personali** Art.. 5, 24, 32-34*

- *.. **un'adeguata sicurezza** dei dati personali, compresa della protezione... **da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali** («integrità e riservatezza»).*
  .. misure tecniche e organizzative... per garantire un livello di sicurezza adeguato al rischio, ...
  - *la pseudonimizzazione e la cifratura;*
  - *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza..*
  - *la capacità di ripristinare tempestivamente ....*
  - *verificare e valutare regolarmente l'efficacia delle misure..*
- *.. si tiene conto in special modo dei rischi .. dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali*
- ***Notifica di violazione all'autorità di controllo** (Art 33)*
- ***Notifica** di violazione agli **interessati** (Art 34)*

Responsabilità Art. 5, 24 e altri

- *Il titolare del trattamento è **responsabile .... e in grado di dimostrare la conformità** («responsabilizzazione»).*
- **Titolari e responsabili hanno l'obbligo di dimostrare la conformità** con i principi della normativa, e quindi l'obbligo di **tracciare le attività di trattamento e la liceità, la raccolta delle informazioni e dei consensi, le attività di gestione, le misure di sicurezza adottate, gli accessi**, ecc..
- Obbligo al "**Registro dei Trattamenti**" (Art.30)
- **Valutazione d'Impatto** (At. 35)

Liceità e **Consenso** (Art 5-8)

- *I dati personali sono: trattati in modo **lecito, corretto e trasparente..** ; **raccolti per finalità determinate, esplicite e legittime...; adeguati, pertinenti e limitati** a quanto necessario ..; conservati in una forma che consenta l'identificazione degli interessati ...;*
- Liceità del trattamento (Art 6)
- Consenso (Art. 7 e 8)

Principi applicabili al trattamento di dati personali

Art. 5, comma 2 - Accountability

[...]

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). (C74) («responsabilizzazione» «accountability»).

Cio' che contraddistingue la gestione della conformità nel GDPR è il principio **che per essere conformi non basta fare ma bisogna dimostrare di aver fatto**

ACCOUNTABILITY

Importante adottare un **processo di Gestione della Privacy** che consenta di mappare, validare e governare le seguenti componenti:

Obbligo di legge	Requisiti per adempiere	Risk Analysis & Privacy Impact Assessment	Misure tecniche ed organizzative adeguate	Evidenze da produrre per ciascuna misura
			Monitoraggio Misure tecniche ed organizzative	Monitoraggio Evidenze

Agenda

- GDPR: overview obblighi e requisiti
- Cosa si deve fare per indirizzare la conformità al GDPR
- Approccio e soluzioni IBM
- Why IBM

Quesiti fondamentali da indirizzare

Quali sono le domande a cui devono rispondere il Titolare e il Responsabile del Trattamento?

1. **Quali dati personali** vengono gestiti?
2. Sono gestiti **in modo consistente con i principi del GDPR**?
3. Sono state **identificate le misure organizzative e tecniche appropriate**?
4. Sono state **applicate** tali misure?
5. Viene **monitorata l'efficacia di tali misure**?
6. Sono state **documentate** tali misure, e vengono **raccolte le evidenze**?

Principali misure di Sicurezza

Best practices ISO 27002

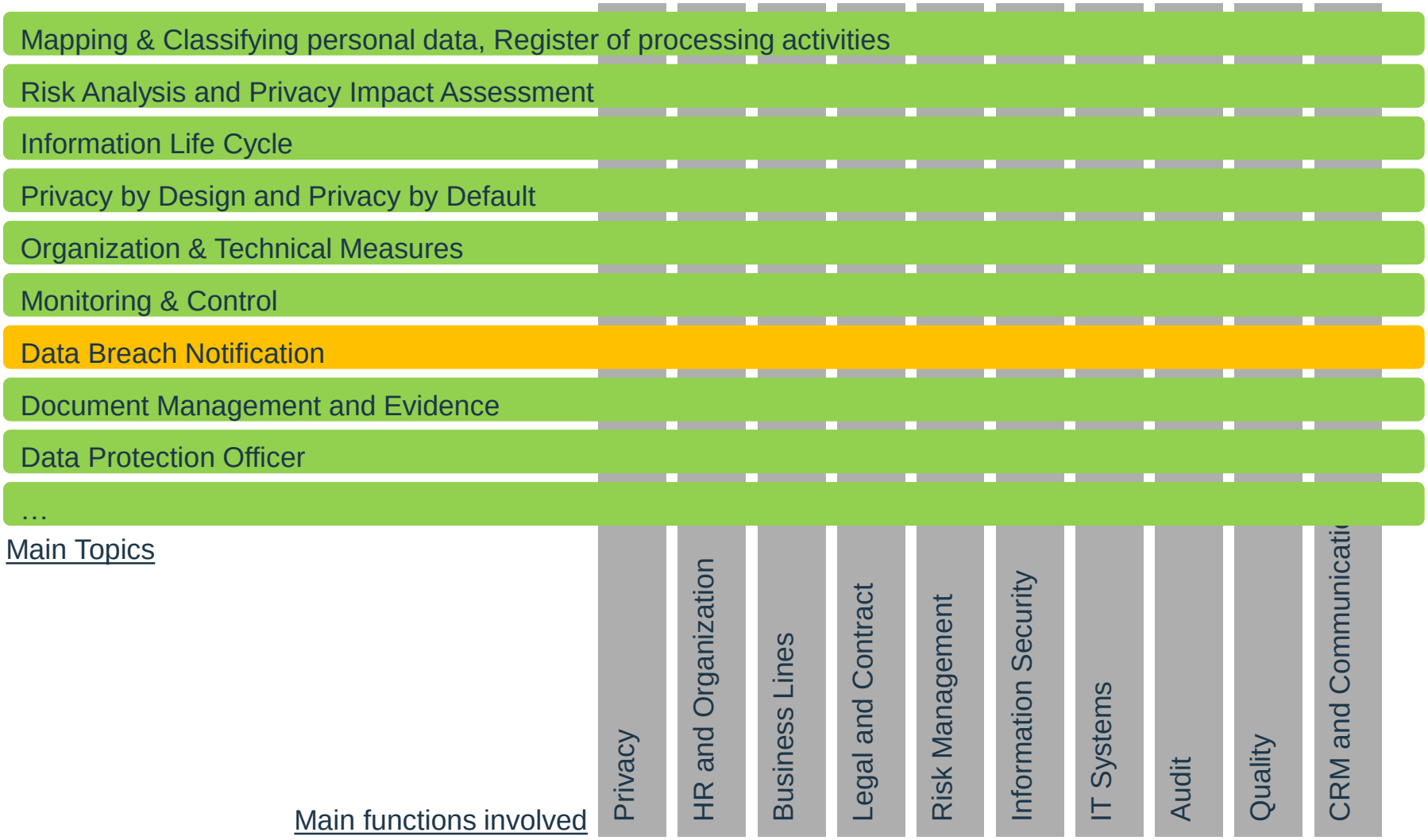
Preventive	ISO 27002
Identity Governance and IAM	Section 9
Data Base Security	Section 9, 12 e 14
Logging and Auditing	Section 12
Network Security	Section 13
EndPoint Security	Section 6, 9 e 11
Data Loss Prevention	Section 8 e 18
Encryption	Section 10
Training	Section 6 e 7
Pseudonymisation	Section 18
Vulnerability of Systems and Applications	Section 12, 14 e 16
Security and Configuration Management	Section 12, 13 e 14

Detection	ISO 27002
Security/Privacy Incident and Event Management	Section 16
Violation Management	Section 16 e 18
Escalation	Section 16 e 18
Notication	Section 6 e 16
Communication	Section 6, 13 e 16

Mitigation/Recovery	ISO 27002
Business Continuity and Disaster Recovery	Section 17
Back Up	Section 12
Redundancy	Section 17

Discipline e ambiti coinvolti

GDPR richiede un approccio multidisciplinare ed il coinvolgimento di gran parte della struttura aziendale



Agenda

- GDPR: overview obblighi e requisiti
- Cosa si deve fare per indirizzare la conformità al GDPR
- Approccio e soluzioni IBM
- Why IBM

La metodologia IBM

IBM ha creato un approccio al GDPR basato sull'integrazione multidisciplinare dei requisiti di adempimento e sugli standard ISO di riferimento

- **IBM Italia ha realizzato un team multidisciplinare**, composto da consulenti esperti di security e privacy, organizzazione aziendale, esperti di tecnologie di Sicurezza e di Data Management (Analytics) al fine di integrare in unico approccio metodologico i servizi e le soluzioni a supporto del GDPR rese disponibili dai brand aziendali
- L'approccio è **scalabile** in funzione del livello di maturità del cliente sulla tematica Privacy
- Il team ha realizzato l'approccio integrato avendo come riferimento i **principali standard ISO in materia di Sicurezza delle Informazioni (famiglia ISO 27001) e Privacy (famiglia ISO 29100)**
- L'approccio multidisciplianre, integrato e basato sugli standard ISO è al momento una caratteristica di **uniqueness** che distingue la proposizione IBM sul mercato rispetto ai competitor
- Tale approccio è **sempre molto apprezzato dai clienti**, in quanto consente di percorrere il cammino verso la conformità normativa puntando anche ad una sua potenziale certificazione ai sensi del GDPR e degli standard ISO, soprattutto per quei clienti che hanno già fatto proprio il modello ISO 27001

Information Security e Data Privacy

L'approccio IBM al GDPR tiene in considerazione le differenze e gli aspetti di correlazione tra Information Security and Data Privacy

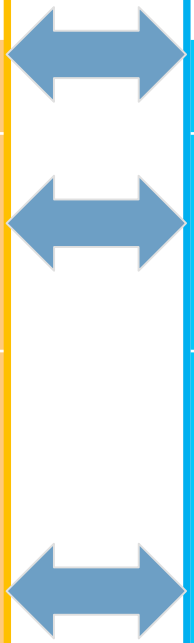
Information Security

L'Information Security è l'iniseme di **tutte le pratiche e i processi in atto per garantire che i dati non siano accessibili o utilizzati da individui o soggetti non autorizzati**. Interesssa una gamma di dati più ampia rispetto ai dati personali, poiché include la protezione di tutte le informazioni e il patrimonio gestito per l'azienda.

- **Security Policies**

- **Security Risk analysis**
- **Security Risk Treatment Plan**
- **Identification of Information Security appropriate organizational and technological Measure**

- **Technical & Organizational Security Measures:**
  - ✓ **Information Security** (Identity and Access Management, SIEM, Encryption, Intrusion Detection Prevention Systems, Firewalls, Antivirus, Access Control Systems, Video Surveillance….)
  - ✓ Security Incident Mgmt & response
  - ✓ Business Continuity and DR



Data Privacy

La Data Privacy **riguarda la definizione di norme che regolano la raccolta e la gestione delle informazioni personali** (sottoinsieme di dati protetti dall' Informazion Security).

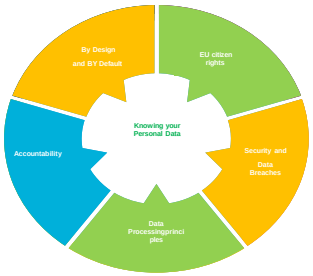
- **Privacy Policies**

- **Privacy Risk Analysis**
- **Privacy Risk Treatment Plan**
- **Identification of Privacy appropriate organizational and technological Measure**

- **Technical & Organizational Privacy Measures:**
  - ✓ **Personal Data Processing measures** (DPO,registro dei Trattamenti, Informativa, Consenso, Applicazione principi del trattamento, dirittti di accesso,, Data breaches monitor&mgmt…….)
  - ✓ **Personal Data Security**: adequate Security measures, encryption, data breach mgmt, by design & by default, ...

Gli Standard ISO

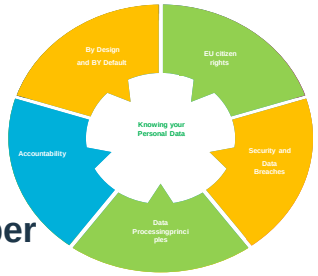
Gli Standard ISO supportano l'adozione dell'Information Security Management System e dei Privacy Management Systems



	Information Security Management System	Privacy Management System
Management System / Framework	ISO/IEC 27001: Information Security Management System	ISO/IEC 29100: Privacy framework
Risk Management	ISO/IEC 27005: Information security risk management	ISO/IEC 29134: Privacy impact assessment
Controls	ISO/IEC 27002: Code of practice for information security controls	ISO/IEC 29151: Code of practice for personally identifiable information protection

L’approccio olistico

IBM ha organizzato le attività GDPR in tre domini, così da coprire l’intero spettro dei requisiti

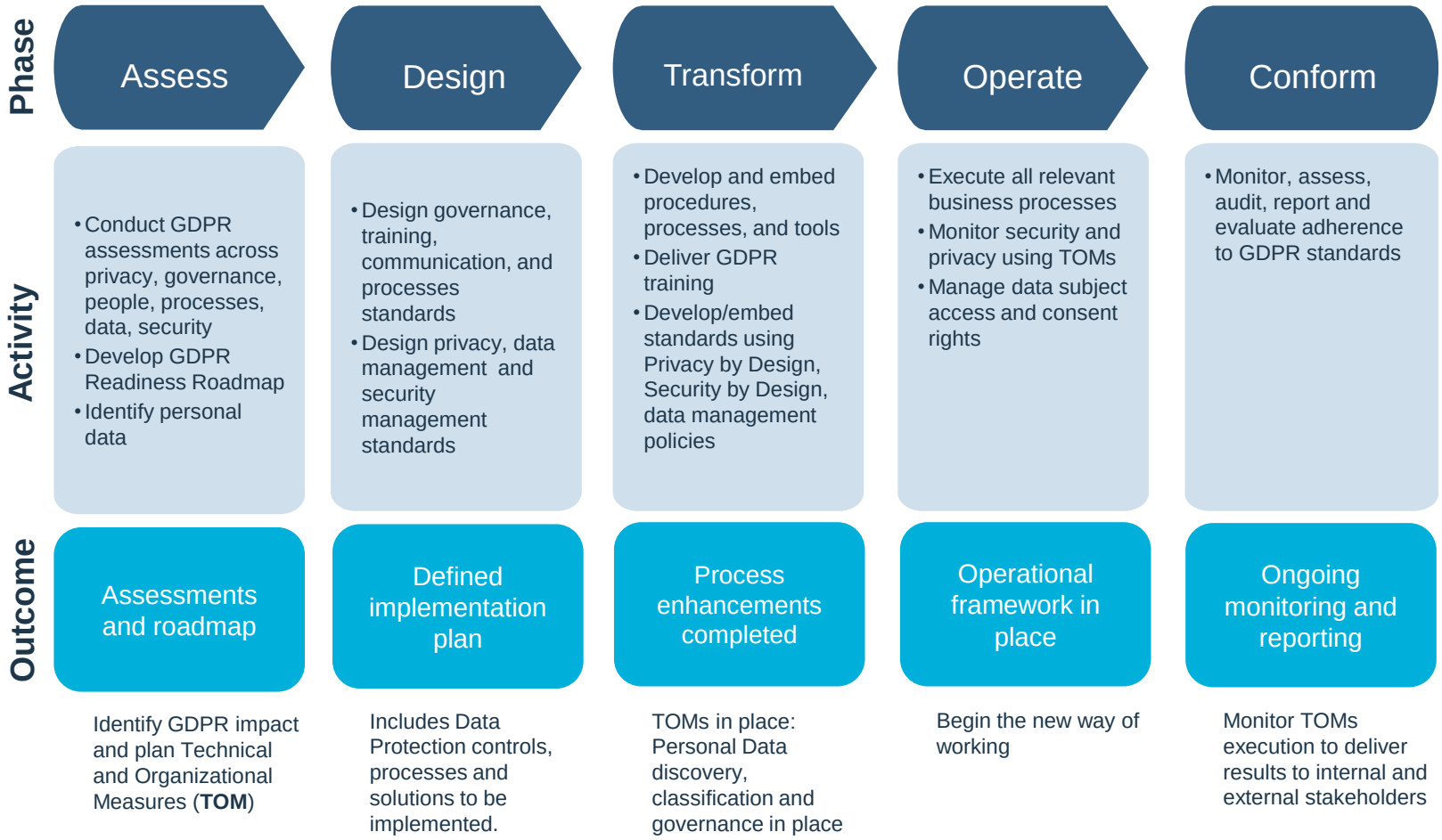


1. **Privacy Compliance Management System, per indirizzare nel complesso la Privacy Accountability:** copre la Privacy Strategy e Risk e Compliance, l’identificazione degli stakeholder Privacy, il processo PDCA, la documentazione e la gestione delle evidenze

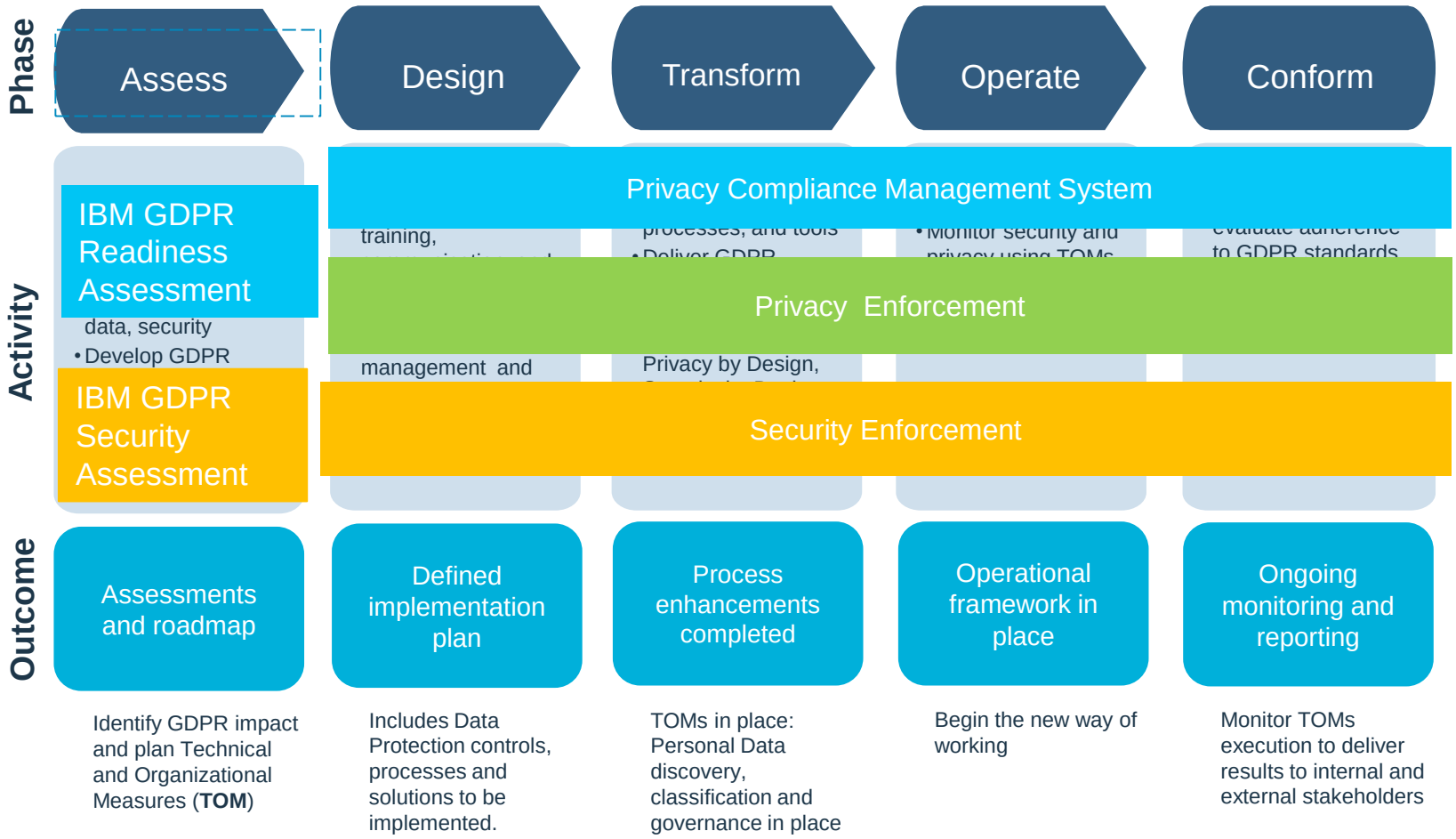
2. **Privacy Enforcement,** inizia dalla Data Discovery basata sulla Analisi dei Rischi Privacy, per indirizzare l’identificazione, disegno, sviluppo, implementazione, gestione e raccolta delle evidenze delle misure e degli adempimenti Privacy specifici appropriati (Notice, Consent, Personal Data Management, Data Subject Rights Management, etc.) che copra anche le applicazioni e gli aspetti di gestione ICT

3. **Security Enforcement**, basata sulla Analisi dei Rischi Security, per indirizzare l’identificazione, disegno, sviluppo, implementazione, gestione e raccolta delle evidenze delle misure adeguate di Security e degli adempimenti specifici (Data Security, Data Breach, Cryptography, etc.)

Le 5 fasi del processo – 1/2

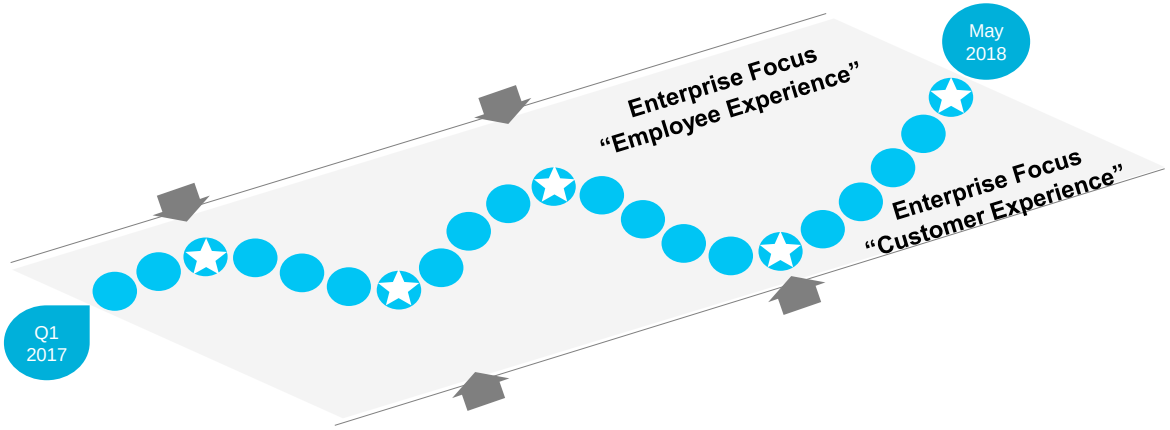


Le 5 fasi del processo – 2/2



La Roadmap

L' approccio IBM è modulare, collegando le soluzioni e servizi a supporto delle iniziative GDPR e scalabile in funzione del livello di maturità del cliente nel percorso verso la conformità al GDPR



***Fase di diagnosi**:*

IBM fornisce una valutazione trasversale per iniziare rapidamente

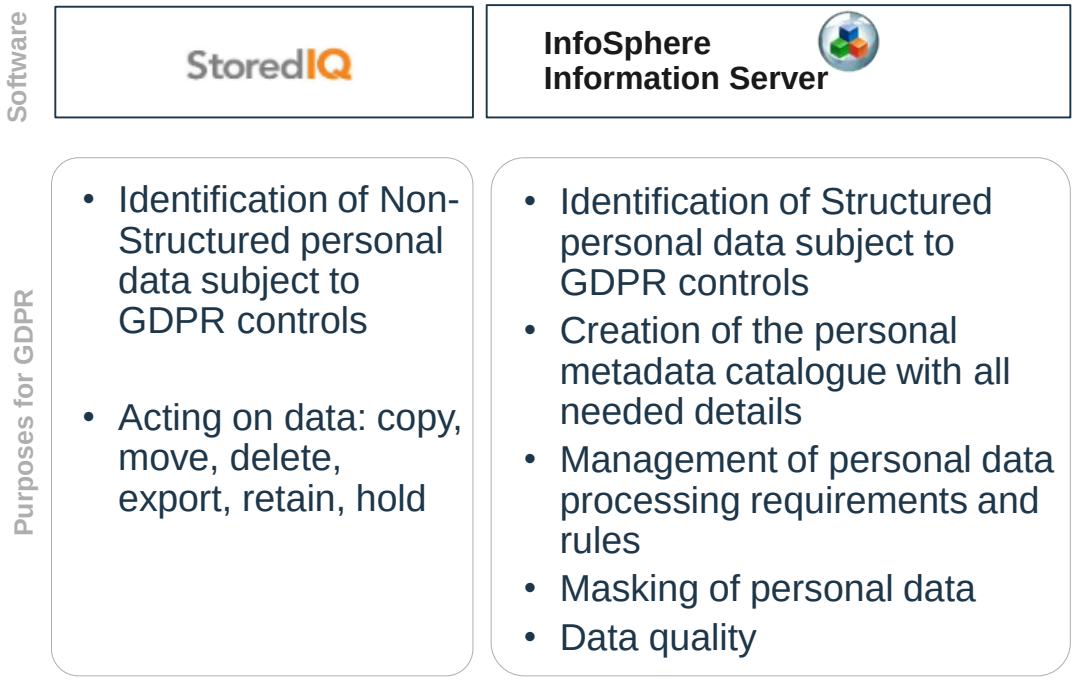
- Una valutazione della maturità della disponibilità ad attuare ogni articolo del GDPR
- Una valutazione di come GDPR sta influenzando i sistemi di gestione Privacy e sicurezza, unita ad ua un gap analysis e relative iniziative
- Una roadmap di implementazione atta ad impostare le priorità

***Fase di definizione**:*

IBM fornisce analisi approfondite all'interno dei domini della Privacy/ Data Management e Sicurezza

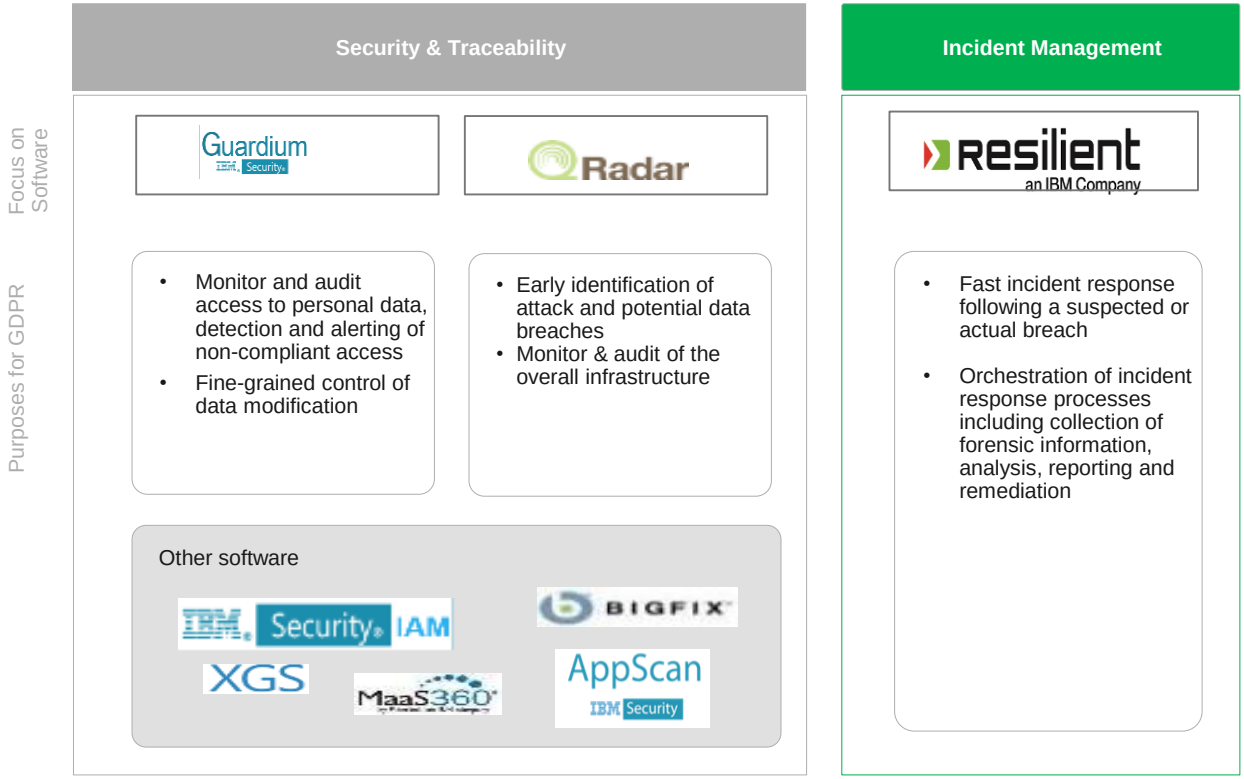
Quick Start analysis	Accelerator Assets
Data Management & Security Software	Managed Delivery Programs

Strumenti per l’identificazione dei dati



Gli strumenti tecnologici proposti da IBM sono in grado di ricercare i dati sensibili nelle piattaforme aziendali e cloud, identificarli, mascherarne la lettura ed interpretazione, gestirne il ciclo di vita supportando l’analisi dei flussi di gestione del dato attraverso l’adozione, quando necessaria, di componenti quali StoredIQ, CaseManager, la suite Infosphere ed Optim, abilitando l’implementazione di soluzioni e tecnologie storage appartenenti alla nuova generazione.

Strumenti per la protezione dei dati



La Sicurezza del Dato richiesta dalla legge è supportata da un primo livello di applicazioni (Compliance Monitoring &Enforcing) che si occupano del far rispettare le politiche di sicurezza del dato nei sistemi aziendali (Guardium), verificare le vulnerabilità delle applicazioni che gestiscono il dato (Appscan) e quindi mantenere un continuo controllo sulla sicurezza aziendale (Qradar) che consente di rilevare le eventuali violazioni al momento in cui si manifestano ed organizzare i processi di gestione di un eventuale incidente (Resilient System).

Agenda

- GDPR: overview obblighi e requisiti per adempiere
- Cosa si deve fare per indirizzare la conformità al GDPR
- Approccio e soluzioni IBM
- Why IBM

Perchè IBM?

I vantaggi della soluzione IBM:

- Il team di consulenza IBM Privacy è un gruppo di professionisti dedicati alla privacy, con un comprovato successo nello sviluppo di soluzioni di data privacy dalle start up, fino alle aziende globali di Fortune 500, comprese quelle dei settori finanziario, assicurativo, retail e automobilistico
- I team di servizi e prodotti sono disponibili a collaborare con il cliente nella progettazione, nello sviluppo e nell'attuazione di un piano di transizione / roadmap in linea con le risorse dei clienti, e i vincoli infrastrutturali o di bilancio
- I prodotti IBM sono utili nel facilitare la transizione (e.g. Guardium, Stored IQ, Identity Governance, Resilient)
- Il nostro vantaggio competitivo: un approccio olistico e consolidato alla preparazione al GDPR

Consulenza sulla privacy + Pianificazione dell’implementazione + Strumenti e Competenza

IBM Commitment to GDPR Readiness Statement

Trust in Data

Data and its protection are becoming increasingly important to individuals and society. Enterprises must earn the public's trust in their ability to steward information. As IBM's long history of security and privacy leadership demonstrates, IBM understands that protecting privacy is essential to gaining trust. IBM was one of the first companies to appoint a Chief Privacy Officer, to develop and publish a genetics privacy policy, to be certified under the APEC Cross Borders Privacy Rules system, and to sign the EU Data Protection Code of Conduct for Cloud Service Providers. Now, IBM is continuing its long-standing leadership in the area of data privacy by responding proactively to the General Data Protection Regulation (GDPR).

IBM Commits to GDPR Readiness

IBM currently complies with privacy laws around the world. IBM is also preparing to comply with the European Union's new General Data Protection Regulation (GDPR) which will go into effect in May 2018. IBM has established a global project to prepare for GDPR, both for our internal processes and for our commercial offerings. IBM recognises that our customers will rely on IBM's offerings and technical assistance to achieve GDPR compliance within their own organisations and IBM is well-positioned to meet this critical need.

As part of its GDPR project, IBM is enhancing its ongoing commitment to privacy by design. IBM is working to embed data protection principles even more deeply into its business processes, with the objective that technical and organisational security measures limit, by default, the amount and use of personal data to what is specifically required. This work will also strengthen controls already in place to limit access to personal data, including with respect to mobile applications that rely on sensible default settings to prevent personal data from being inadvertently shared with others.

IBM is committed to providing our clients and partners with innovative data privacy, security and governance solutions to assist them on their journey to GDPR compliance.

Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings to support your compliance journey here.

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM