Accenture Security

General Data Protection Regulation (GDPR)

Andrea Agosti
Mariangela Fierro

Milano, 19 Dicembre 2016

accenture

Obiettivi

Comprendere i requisiti della GDPR e le principali novità introdotte

Identificare i principali impatti tecnici e organizzativi

Proporre una roadmap / piano di azione per l'adeguamento normativo

General Data Protection Regulation overview

Obiettivi, timeline e principali novità introdotte

Obiettivi

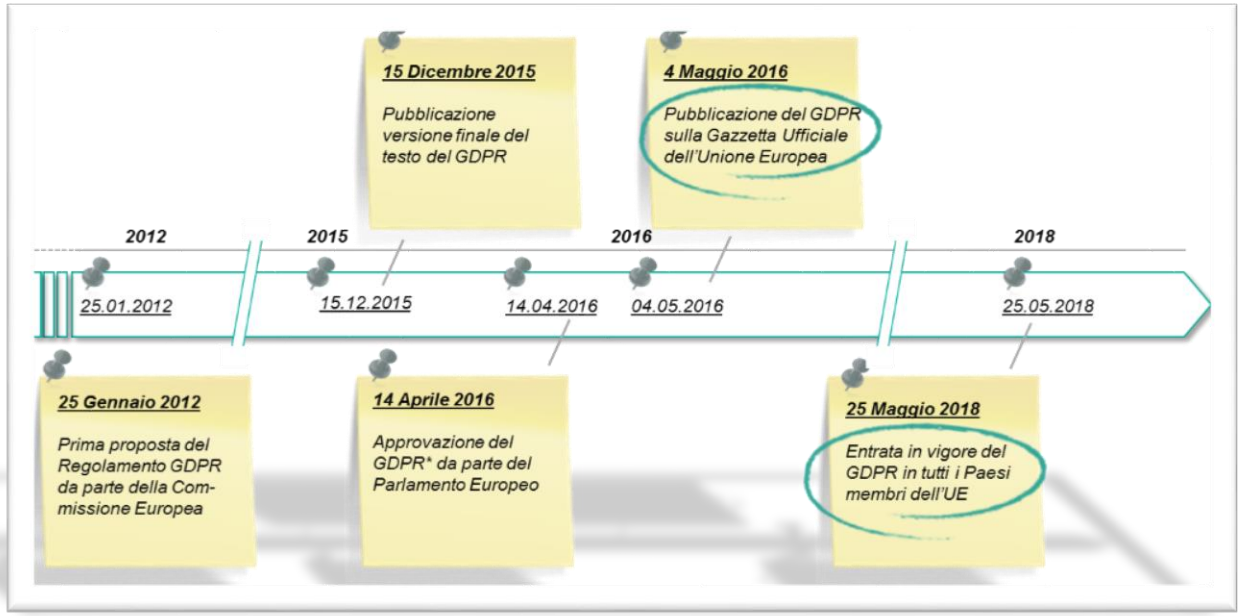
La nuova normativa Europea in tema di *Data Protection* (Regolamento UE 2016/679) ha l'obiettivo di:

- **Garantire una maggior tutela della Privacy** in tutti i Paesi membri dell'UE
- **Armonizzare le diverse normative nazionali** per favorire lo sviluppo di un **unico mercato digitale europeo**

Quando

- Il **4 maggio 2016** è stato **pubblicato** sulla Gazzetta Ufficiale dell'Unione Europea il nuovo Regolamento 2016/679 (che abroga la Direttiva 95/46/CE) sulla protezione dei dati personali e la libera circolazione dei dati personali, che si **applicherà a decorrere dal 25 maggio 2018**
- Il Regolamento **è direttamente applicabile** e vincolante in tutti gli Stati dell'Unione Europea

La storia e le tappe



General Data Protection Regulation overview

Motivazioni alla base della riforma del framework EU di Data Protection

	Trend di Mercato	*Principali Evidenze*	*Obiettivi del GDPR*
1 **Digital Single Market**	▪ L'istituzione di un unico mercato digitale europeo richiede **l'armonizzazione delle norme nazionali** di Data Protection	**90%** *Cittadini europei che chiedono **uguali diritti di data privacy,** indipendentemente da dove i dati vengano trattati** **2.3 Bln** *Risparmi per il **business** in relazione alla **frammentazione** attuale in **28 normative** nazionali*	▪ Armonizzare le diverse normative esistenti in materia di Data Priotection e Privacy, garantendo la diretta applicazione di in un unico Regolamento in tutta l'Unione Europea
2 **Cyber Risk**	▪ Il trend crescente di **attacchi informatici**, sempre più sofisticati, richiede **livelli maggiori di protezione dei dati sensibili** e maggiori tutele per gli interessati	**300 Mln** ***Malware** creati nel 2015** **+24%** *N° di **data breaches** 2015 vs 2014**	▪ Diminuire il rischio di attacchi informatici, che hanno come obiettivo il furto o il danneggiamento dei dati personali
3 **Big Data e Cloud**	▪ **Grandi moli di dati e nuove tecnologie** per effettuare elaborazioni (i.e. *Big Data Analytics*) oltre che archiviare i dati (i.e. *Cloud*) vengono usati all'interno dei **processi di *decision-making***	*% di dati digitali archiviati nei Cloud sul tot. di dati delle organizzazioni** **20%** ***nel 2014*** **40%** ***Entro il 2020***	▪ Aumentare il livello di confidenza rispetto ai trattamenti di dati personali, con particolare riguardo ai servizi online e alle nuove tecnologie

Accenture Security

(*) Fonte: "Why we need a Digital Single Market", European Commission factsheet, Maggio 2015
(**) Fonte: "Internet Security Threat Report", Symantec, Aprile 2015, Volume 20

General Data Protection Regulation overview

At a glance

- **Nuovi e rafforzati diritti per gli interessati** (ad esempio diritto di **trasparenza**, **opposizione**, **all'«oblio»** e alla **portabilità dei dati**)
- Nuovi obblighi e rafforzamento dell'**accountability** in carico ai soggetti che trattano dati personali (in primis, **data protection impact assessment, data protection by default e by design, istituzione della figura del Data Protection Officer, data breach notification**)

Focus delle prossime slide

- **Inasprimento del regime sanzionatorio amministrativo** in caso di violazioni dei dati (fino a € 20Mln al 4% del fatturato globale), con possibilità di sanzioni penali lasciate ai singoli stati
- Promozione di **schemi di certificazione** e **codici di condotta** per dimostrare la conformità ad alcuni aspetti del Regolamento (ad esempio bollino blu privacy)
- Definizione di una **Commissione Europea** per la protezione dei dati che coordinerà le autorità sovrintendenti (European Data Protection Board)
- Applicazione a tutti i soggetti residenti in UE, indipendentemente dal fatto che il trattamento sia svolto **all'interno della UE o al di fuori dell'UE**

General Data Protection Regulation overview

Principali novità per i soggetti che trattano dati personali

Ambito	Principali novità
Rafforzamento principi e diritti per gli interessati	1) Rafforzamento delle condizioni per garantire un **consenso informato**, **libero** e **verificabile** 2) Incremento della **trasparenza** su **informazioni**, **modalità** per l'**esercizio** dei **diritti** 3) Ampliamento delle **informazioni** sui **trattamenti** e possibilità di **accesso** ai **dati personali** 4) Cancellazione (cosiddetto "**oblio**") dei **dati personali** conservati da un titolare 5) Portabilità e **s**emplificazione del **trasferimento dei dati** personali tra **differenti titolari** 6) Possibilità di **opposizione** rispetto a **determinati trattamenti**, tra cui **marketing diretto** 7) Sospensione dai **processi decisionali automatizzati**, specie nel caso della **profilazione**
Incremento degli obblighi per titolari e responsabili	8) Rafforzamento dell'**accountability** rispetto alla compliance sulle responsabilità assegnate 9) Registrazione e mantenimento **di adeguata documentazione** sui trattamenti effettuati 10) Adozione di misure per la **protezione dei dati personali e la sicurezza dei trattamenti** 11) Procedure di **notifica ad Autorità e interessati** delle violazioni sui dati personali 12) Necessità di esecuzione di una **valutazione d'impatto** sui trattamenti ad alto rischio 13) Nomina del **responsabile della protezione dei dati personali** (Data Protection Officer) 14) Introduzione del concetto di protezione dei dati by design **(*Privacy By Design*)** 15) Introduzione del concetto di protezione dei dati by default **(*Privacy By Default*)**

Sfide ed Impatti

Le misure tecniche ed organizzative richieste dal GDPR (1 di 2)

Aree di impatto	***Azioni «To Do»***
 **Compliance**	✓ Definire o rivedere il modello di **data privacy**, in ottemperanza alle responsabilità derivanti dal nuovo regolamento ✓ Istituire un **registro dei trattamenti Privacy** ✓ Definire o rivedere l'impianto documentale, in termini di policy e procedure per il rispetto dei requisiti di **accountability** ✓ Rivedere le informative Privacy per la **raccolta dei consensi** e garantire la trasparenza verso i clienti ✓ Definire i controlli e la reportistica necessaria per il **monitoring nel tempo dello stato di conformità**
 **Organizzazione/Processi**	✓ Rivedere e razionalizzare i processi per la gestione del consenso e le **modalità di richiesta degli interessati** (oblio, accesso ai dati, portabilità dei dati) ✓ Rivedere il modello organizzativo per la **nomina del DPO** ✓ Definire un piano adeguato di **training ed awareness verso i dipendenti** ✓ **Definire il mapping dei dati personali** e dei flussi degli stessi verso le terze parti ✓ Supportare l'integrazione di una **metodologia unica di DPIA**, con il supporto delle funzioni Security e Privacy
 **Contrattualistica**	✓ Rivedere i **contratti con le terze parti** per l'inserimento della clausola di conformità al GDPR in ambito contrattuale ✓ Rivedere e/o definire un set di regole contrattuali per il **trasferimento dei dati personali** tra società del gruppo ✓ Migliorare le norme vincolanti d'impresa e adottarne di nuove - se necessario - in tema di trasferimento dei dati

Sfide ed Impatti

Le misure tecniche ed organizzative richieste dal GDPR (2 di 2)

Aree di impatto	***Azioni «To Do»***
Information Security	✓ Definire ed implementare **le misure di sicurezza** che devono essere implementate per assicurare la protezione dei dati personali (protection at rest / in use/ in motion) e prevenire il **data leakage** ✓ Definire ed implementare le misure tecniche per la **pseudonomizzazione** o **cifratura** dei dati ✓ Identificare e classificare i dati personali all'interno dell'azienda e definire i controlli da applicare in base alla classificazione ✓ Definire la metodologia e le misure per garantire la protezione dei dati fin dalla fase di progettazione (***Privacy By Design***), senza eccesso di trattamento (***Privacy by Default***) ✓ Supportare l'esecuzione della valutazione dei possibili impatti, attraverso la **Data Protection Impact Assessment** (DPIA), per i trattamenti definiti ad alto rischio ✓ Rivedere e/o implementare le misure di sicurezza adeguate per la detection di eventuali incidenti e la definizione del processo di **Data Breach notification**
Information Technology	✓ Supportare la **mappatura dei dati personali** sui sistemi informativi ed i flussi verso i sistemi esterni ✓ Disegnare ed implementare **misure di cancellazione** dei dati su tutti gli applicativi che trattano dati personali ✓ Rivedere i modelli applicativi per **supportare la cifratura dei dati** – laddove possibile ✓ **Sviluppare procedure IT per il tracciamento dei consensi** e delle richieste degli interessati ✓ Disegnare ed implementare delle procedure informatiche per rispondere alle **richieste degli interessati** (ad es. richiesta di portabilità, accesso ai dati)

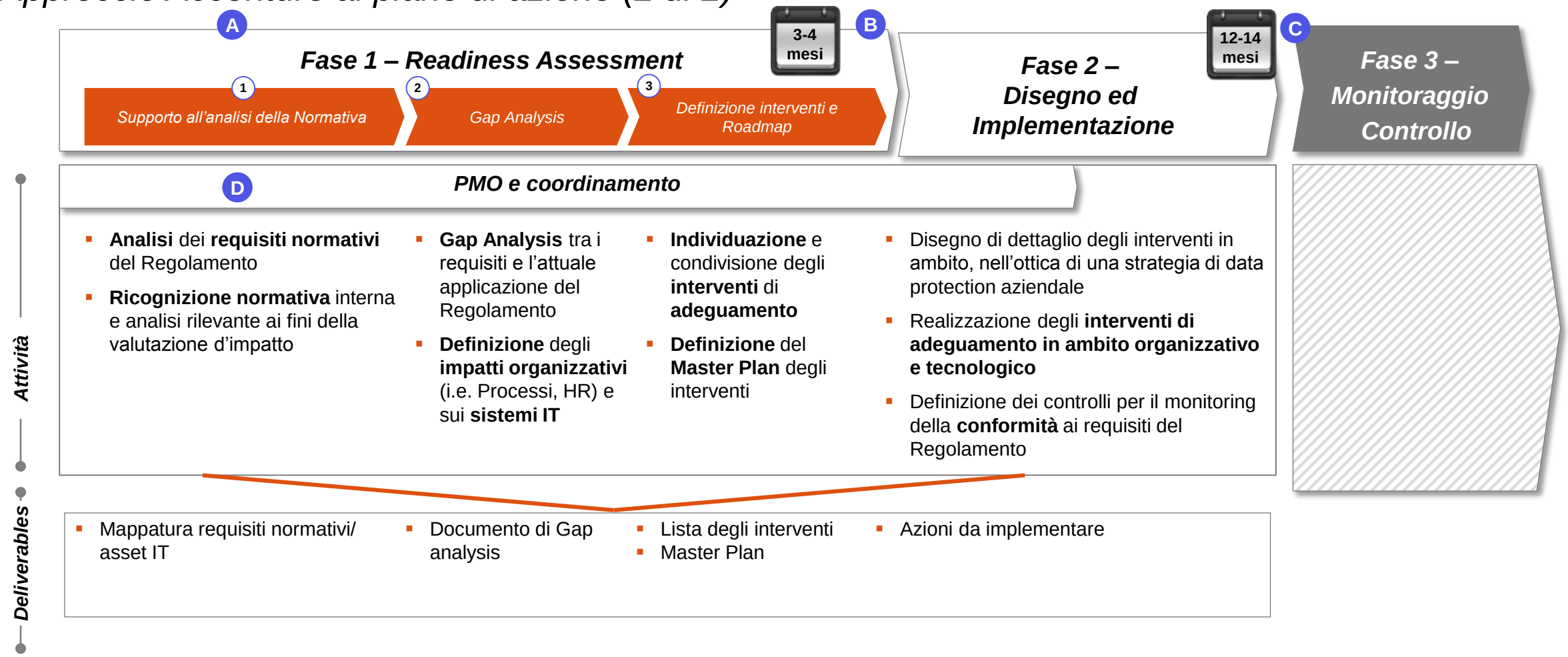
Piano di azione

Approccio Accenture al piano di azione (1 di 2)

Accenture Security

Piano di azione

Approccio Accenture al piano di azione (2 di 2)



Piano di azione

Focus sulla prima fase di lavoro – fasi del Readiness Assessment

A

Fase 1 – Readiness Assessment

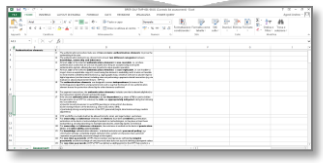
1. *Supporto all'analisi della Normativa*
2. *Gap Analysis*
3. *Definizione interventi e Roadmap*

Attività

Deliverables

Supporto all'analisi della Normativa

- **Raccolta ed analisi** della documentazione aziendale disponibile
- Prima valutazione dei circa **99 requisiti** contenuti nel Regolamento Europeo per valutarne l'applicabilità nel contesto aziendale.



Gap Analysis

- **Esecuzione interviste** con le funzioni aziendali responsabili dei differenti ambiti (Sicurezza, IT, Risk Management, Legale,Organizzazione, Audit, Comunicazione)
- **Diagnostico della situazione** aziendale in relazione ai requisiti del Regolamento (gap analysis)
- **Identificazione degli scostamenti** e definizione dei relativi **interventi di adeguamento**

Definizione interventi e Roadmap

- Predisposizione di un **Piano di quick-win** con gli interventi da realizzare nel breve, per indirizzare eventuali aree di scopertura rispetto ai requisiti normativi
- Predisposizione **Master Plan** per organizzazione complessiva degli interventi identificati

Piano di azione

Focus sulla seconda fase di lavoro

L'implementazione delle misure di sicurezza, che consentono all'organizzazione di evitare diffusione accidentale e non autorizzata dei dati personali, deve essere programmata e pianificata seguendo tre fasi:

Fase

A	B	C
Data Inventory e Classificazione	**Data Protection Strategy**	**Dalla Strategia al Rollout**

Descrizione

- **Censimento e identificazione** dei dati personali in ambito, attraverso la mappatura di:
  - **Processi** che consentono il trattamento di dati personali
  - **Supporti informatici e non** per il trattamento dei dati personali
  - **Flussi di scambio** tra i supporti informatici
- Classificazione dati in base alla valutazione di impatti in termini di **confidenzialità, integrità e disponibilità dei dati**
- **Inventario** *retention* dei dati

- Valutazione e disegno della strategia di Data Protection per l'identificazione delle misure di sicurezza dei dati per la **protezione degli stessi da accessi e/o modifiche accidentale o non autorizzate, sulla base della tipologia di dati identificati**
  - Protezione dei dati ***at rest*** (es. *storage, database*) con soluzioni di sicurezza dei database, NAS (es. *data masking, obfuscation, db encryption, database auditing monitoring*)
  - Protezione dei dati ***in transito*** (es. *e-mail security, encryption*)

- Identificazione di un pilota di applicazioni / dati per l'implementazione delle misure di sicurezza identificate, prioritizzandoli su base rischio
- Estensione del rollout
- Definizione e messa a terra del modello di **Data Governance** finalizzato al governo dei dati aziendali e delle politiche di enforcement

Piano di azione

Focus su mappa tecnologica a supporto dell'implementazione

Applicazioni e Sistemi IT

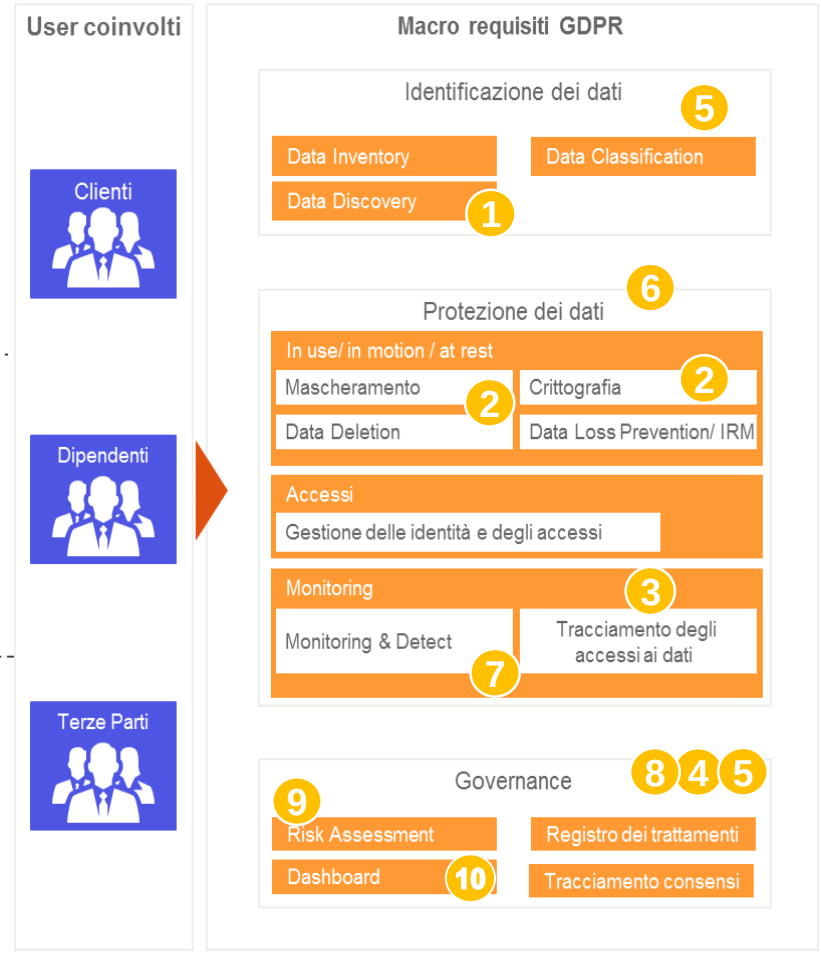
1. **Valutazione dei periodi di retention dei dati** personali e sviluppo di procedure di cancellazione ad hoc
2. **Adeguamento degli applicativi** per l'abilitazione delle funzionalità di masking ed encryption
3. **Sviluppo e/o integrazione di access log** per il tracciamento delle operazioni effettuate sui dati
4. **Implementazione di processi** di *privacy by design* e *by default* nel ciclo di sviluppo applicativo

Data Protection

5. **Identificazione e classificazione dei dati personali sui sistemi IT / base dati**
6. **Sviluppo e/ o rafforzamento delle misure di sicurezza** per la prevenzione della perdita, alterabilità e disponobilità dei dati (data loss prevention, IRM, encryption, masking)
7. **Revisione e/o disegno** di un processo di data breach

Diritti degli interessati

8. **Identificazione e revisione dei processi di raccolta del consenso,** con eventuale introduzione di automatismi di storicizzazione
9. **Assessment applicativo per la valutazione dello** stato di resilienza delle applicazioni e della security posture
10. **Sviluppo di processi e procedure** per il soddisfacimento delle richieste degli interessati (es.diritto alla portabilità e all'oblio)



THANK YOU

Accenture Security