
rethinking the future together

# Il GDPR e le opportunità offerte dalle soluzioni di sicurezza gestita

# DEFINIZIONI – TITOLARI E RESPONSABILI

I titolari (controller) del trattamento dei dati personali

- sono persone fisiche, persone giuridiche, autorità pubblica o altro organismo
- determina le finalità, le condizioni e gli strumenti per il trattamento dei dati personali.

I responsabili (processor) del trattamento dei dati personali

- sono persone fisiche, persone giuridiche, autorità pubblica o altro organismo
- elaborano i dati per conto dei titolari del trattamento

# DEFINIZIONI – TRATTAMENTO

Il trattamento (processing) dei dati personali

- è qualsiasi operazione, o insieme di operazioni, che viene eseguita su dati personali o su set di dati personali, anche con mezzi automatizzati, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, l'archiviazione, l'adattamento o l'alterazione, il recupero, la consultazione, l'uso, la divulgazione mediante trasmissione, diffusione, allineamento o combinazione, restrizione, cancellazione o distruzione.

# DEFINIZIONI – DATI PERSONALI

I dati personali sono informazioni che possono essere utilizzate da sole o con altre informazioni per identificare l'utente come persona. Ad Esempio:

- Nome e Cognome
- Data di nascita
- Indirizzo di casa
- Indirizzo email
- Numero di telefono
- Codice Fiscale
- Numero di passaporto
- indirizzo IP (in genere quando collegato ad altre informazioni)
- Targa automobilistica
- Patente di guida
- Dati Biometrici o calligrafici
- La documentazione sanitaria
- Dati bancari

# DEFINIZIONI – DATA BREACH

Per violazione dei dati personali si intende la distruzione, perdita, alterazione, divulgazione non autorizzata o accesso, in modo accidentale o illecito, ai dati personali trasmessi, conservati o comunque trattati.

- Violazioni dall'interno – Gestione dei sistemi interni
- Violazioni dall'esterno – Gestione del 'perimetro'

# PRINCIPI FONDAMENTALI – ACCOUNTABILITY (ART. 24)

Il titolare del trattamento deve attuare le adeguate misure tecniche e organizzative per garantire e dimostrare che il trattamento (processing) è effettuato in conformità del regolamento. Tali misure saranno riesaminate e aggiornate se necessario.

# PRINCIPI FONDAMENTALI – DATA PROTECTION (ART. 25)

## BY DEFAULT

Il titolare del trattamento deve assicurare che vengono trattati i soli dati personali necessari per le finalità previste e per il periodo strettamente necessario a tali fini.

## BY DESIGN

Il titolare del trattamento deve attuare le adeguate misure tecniche ed organizzative sia all'atto della progettazione che dell'esecuzione del trattamento.

# PRINCIPI FONDAMENTALI – SICUREZZA DEL TRATTAMENTO (ART. 32)

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 e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono:

- 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

# PRINCIPI FONDAMENTALI – REGISTRO DELLE ATTIVITA' (ART. 30)

Ogni Titolare del trattamento deve tenere un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro deve contenere tutte le seguenti informazioni:

- gli estremi del Titolare o del Responsabile del trattamento e, ove presente, del Responsabile della protezione dei dati
- le finalità del trattamento
- una descrizione delle categorie di interessati e di dati oggetto del trattamento e delle categorie di destinatari cui i dati vengono comunicati
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative (riferite all'ART. 32)

# PRINCIPI FONDAMENTALI – REGISTRO DELLE ATTIVITA' (ART. 30) CONT.

Il Responsabile del trattamento tiene un registro di tutte le categorie di attività relative al trattamento svolte per conto di un Titolare del trattamento e deve contenere:

- gli estremi del Responsabile del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento e, ove applicabile, del Responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative (riferite all'ART. 32)

# PRINCIPI FONDAMENTALI – REGISTRO DELLE ATTIVITA' (ART. 30) CONT.

- I registri sono tenuti in forma scritta, anche in formato elettronico.
- Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
- Gli obblighi citati non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10

# PRINCIPI FONDAMENTALI – BREACH NOTIFICATION (ART. 33 E 34)

Il titolare del trattamento deve segnalare una violazione dei dati all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro e non oltre le 72 ore successive dalla scoperta della violazione, se questa non arreca un rischio per i diritti e le libertà delle persone interessate. (ART. 33)

Quando la violazione dei dati personali può provocare un rischio elevato ai diritti e le libertà di un soggetto, il titolare del trattamento deve comunicare la violazione al diretto interessato senza ingiustificato ritardo. (ART. 34)

# DA DOVE INIZIARE – I DATI

LE AZIENDE DEVONO CONSIDERARE:

- Di quali dati personali sono titolari
- Dove i dati personali vengono memorizzati
- Come i dati personali vengono memorizzati
- Chi può accedere ai dati personali
- Come si ottiene l'accesso ai dati personali
- Chi sta monitorando i dati personali
- Come i dati personali sono accessibili su richiesta
- Come dati personali possono essere cancellati su richiesta

# AZIENDE VS SICUREZZA – OBIETTIVO

Data Protection By Design

Data Protection By Default

Sicurezza del trattamento

# AZIENDE VS SICUREZZA – IN PRATICA

## A COSA SONO ESPOSTE:

- PROBLEMATICHE COMPLESSE E DINAMICHE
- GESTIONE E CONTROLLO COSTANTI
- FORMAZIONE SPECIFICA E COSTANTE

## SU COSA SI CONCENTRANO:

- IL CORE BUSINESS NON E' LA SECURITY
- LE RISORSE INTERNE SONO IMPEGNATE PER IL CONSEGUIMENTO DEL BUSINESS

# INFRASTRUTTURA DI SECURITY

## COSA COMPORTA UN'INFRASTRUTTURA DI SECURITY

- ASSET MANAGEMENT
- ALERT MANAGEMENT
- INCIDENT MANAGEMENT
- PROBLEM MANAGEMENT

# ASSET MANAGEMENT

- CESPITI
- PHASE OUT
- LICENSING
- UPGRADE (Major Release, Patch Release)
- CONFIGURATION
- GUASTO

# ALERT MANAGEMENT

GLI ALERT SONO SEGNALAZIONI E POSSONO ESSERE DI DUE TIPI:

GENERATI DAI SISTEMI

- Syslog o messaggi strutturati inviati ad un collettore
- Contengono informazioni che vanno interpretate e correlate
- Indicano lo 'stato di salute dell'infrastruttura'

GENERATI DAL GESTORE

- Indicano condizioni di rischio certe o da accertare

# INCIDENT MANAGEMENT

INCIDENT: qualsiasi evento che non fa parte dell'operatività standard di un servizio e che ne può compromettere lo stato e la fruibilità.

GESTIONE DELL'INCIDENT

- analisi e diagnosi
- soluzione e ripristino

# PROBLEM MANAGEMENT

GESTIONE DEGLI INCIDENT NEL LUNGO TERMINE

- Minimizzare l'impatto degli incident
- Prevenire la ricorrenza degli incident
- Determinare le root causes

# TEST SPA – TECHNICAL SUPPORT

## I SERVIZI OFFERTI

- Technical Support
- Configuration Management & Compliance
- Log Management & Reports
- Security Monitoring & Alerting
- Proactive Security Monitoring & Alerting (SIEM)
- Security Assessment (Vulnerability Assessment e Penetration test)
- Vulnerability Assessment
- Penetration Test
- Change Management

# TEST SPA – TECHNICAL SUPPORT

- SERVIZIO BASE
- ASSISTENZA TECNICA DI 2° LIVELLO
- GESTIONE DEI MALFUNZIONAMENTI DELL'INFRASTRUTTURA
- GESTIONE DEI RAPPORTI CON IL VENDOR
- TELEASSISTENZA / ONSITE
- DEFINIZIONE DEGLI SLA

# TEST SPA – CONFIGURATION MANAGEMENT & COMPLIANCE

- GARANTISCE L'ALLINEAMENTO DELLE REGOLE DEL FIREWALL, E DEGLI ALTRI DISPOSITIVI DI SECURITY, A QUELLE CHE SONO LE DIRETTIVE AZIENDALI (SECURITY POLICY)

- VERIFICA DELLA CONFORMITA' DELLE MODIFICHE (CHANGE) NEL RISPETTO DELLE SECURITY POLICIES AZIENDALI E DELLE BEST PRACTICE.

# TEST SPA – LOG MANAGEMENT & REPORTS

## LOG

- GESTIONE DELLE SEGNALAZIONI GENERATE DALL'INFRASTRUTTURA
- LOG COLLECTOR
- TROUBLESHOOTING REAL TIME and HISTORICAL

## REPORTING

- ON DEMAND
- SCHEDULED
- CUSTOM

# TEST SPA – SECURITY MONITORING & ALERTING

## MONITORING

- CONTROLLO E ANALISI COSTANTE DEGLI EVENTI
- IDENTIFICAZIONE DELLE VIOLAZIONI
- IDENTIFICAZIONE DELLE MINACCE POTENZIALI

## ALERTING

- SEGNALAZIONE DELLE VIOLAZIONI
- SEGNALAZIONE DELLE CONDIZIONI DI RISCHIO
- PUO' GENERARE DEI CHANGE MANAGEMENT

# TEST SPA – PROACTIVE SECURITY MONITORING & ALERTING (SIEM)

- CORRELAZIONE DEGLI EVENTI
- PREDISPOSIZIONE DI UN SISTEMA SIEM (*Security Information and Event Management)*
- ALERTING COME NEL CASO NON PROACTIVE

# TEST SPA – SECURITY ASSESSMENT

## VULNERABILITY ASSESSMENT

- CHECK PERIODICO DEI SISTEMI PER IL'INDIVIDUAZIONE DI VULNERABILITA' NOTE (BUG OS, BUG APPLICATIVI, …)
- GENERAZIONE DI REPORT CON INDICAZIONE DI CRITICITA' E AZIONI CORRETTIVE

## PENETRATION TEST

- ONE TIME / PERIODICO
- SCAN E TENTATIVI DI HACKING DEI SISTEMI
- STRUMENTI E COMPETENZE
- GENERAZIONE DI REPORT CON INDICAZIONE DI CRITICITA' E AZIONI CORRETTIVE

# TEST SPA – SECURITY CHIAVI IN MANO

- SOLUZIONE TARATA SULLE REALI ESIGENZE (VALUTAZIONE DEL LIVELLO DI RISCHIO)
- NESSUN ONERE INFRASTRUTTURALE
- CANONE DI SERVIZIO (OPEX vs CAPEX)
- CONTROLLO COSTANTE

# GRAZIE

www.testspa.com