GDPR E PROTEZIONE DEI DATI NELLE INFRASTRUTTURE DI RETE

COSA È IL GDPR?

GENERAL DATA PROTECTION REGULATION

È un regolamento europeo pienamente applicato dal 25 maggio 2018 in tutti gli Stati membri dell'Unione Europea. Il suo obiettivo è rafforzare e unificare la protezione dei dati personali delle persone fisiche all'interno dell'UE, ogni persona può decidere in modo più consapevole e diretto come e da chi i propri dati vengono utilizzati. Per le imprese invece è servito per ridurre la burocrazia e facilitare la gestione dei dati personali.

Il GDPR si applica a qualsiasi organizzazione, anche con sede fuori dall'UE, che tratta dati personali di residenti nell'Unione Europea. I dati personali, secondo il regolamento, sono tutte le informazioni che riguardano una persona fisica identificata o identificabile, come nomi, indirizzi email, dati biometrici, indirizzi IP, informazioni sanitarie e altri dati che possono, anche indirettamente, portare all'identificazione di un individuo.

Il regolamento introduce principi fondamentali come trasparenza, liceità, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, oltre a stabilire diritti specifici per gli interessati (come diritto di accesso, rettifica, cancellazione, portabilità dei dati e opposizione al trattamento).

TECNICA DELLA PRIVACY BY DESIGN

-La tecnica prevede che la tutela della privacy non deve essere un'aggiunta successiva, ma una componente fondamentale e preventiva, incorporata sin dall'inizio nello sviluppo di qualsiasi soluzione digitale o organizzativa, quindi impone di integrare la protezione dei dati personali fin dalla fase di progettazione di un sistema, prodotto, servizio o processo, e durante tutto il loro ciclo di vita.

-I titolari e responsabili del servizio devono adottare misure tecniche e organizzative per minimizzare i rischi per la privacy, garantendo trasparenza, limitazione delle finalità, minimizzazione dei dati, integrità e riservatezza. Si tratta di un approccio volto a proteggere i dati personali evitando problemi prima che si verifichino.

PROTEZIONE DEI DATI IN TRANSITO E A RIPOSO

La protezione dei dati personali richiede misure specifiche sia per i dati a riposo, cioè quelli archiviati su dispositivi o server, sia per i dati in transito, ovvero quelli trasferiti tra sistemi.

• I dati a riposo si proteggono principalmente attraverso la crittografia, che rende i dati illeggibili a chi non è autorizzato, insieme a backup sicuri e aggiornamenti costanti per prevenire vulnerabilità.

• Per i dati in transito, è fondamentale utilizzare la crittografia end-to-end (metodo di sicurezza che protegge le comunicazioni) e protocolli sicuri come TLS/HTTPS, che garantiscono la riservatezza durante la trasmissione.

GESTIONE TECNICA DEI DATA BREACH

La gestione tecnica di un data breach (violazione dei dati personali) inizia con la rilevazione dell'incidente, cioè il momento in cui si scopre che dati personali sono stati accidentalmente o illegalmente accessi, divulgati, modificati o persi. Dopo di che, bisogna contenere l'incidente adottando misure per limitare i danni, come bloccare gli accessi non autorizzati.

Successivamente, si effettua una valutazione del rischio per capire quanto la violazione possa influire sui diritti e sulla privacy delle persone coinvolte. Se il rischio è considerato elevato, il GDPR impone di notificare l'Autorità Garante per la protezione dei dati entro 72 ore dalla scoperta dell'incidente.

Dopo la notifica si procede con un'indagine approfondita e tutto il processo deve essere documentato accuratamente, mantenendo traccia di ogni fase per garantire trasparenza e migliorare continuamente la sicurezza dei dati.

ARCHITETTURE A SUPPORTO DEI DIRITTI DEGLI INTERESSATI

Le architetture a supporto dei diritti degli interessati nel contesto GDPR sono progettate per garantire che le persone possano esercitare i propri diritti, come accesso, rettifica, cancellazione e opposizione al trattamento dei dati personali. Le architetture devono implementare il principio di privacy by design, integrando la protezione dei dati fin dalla progettazione dei sistemi, garantendo che vengano trattati solo i dati necessari e che siano facilmente accessibili e modificabili dagli interessati.

DIRITTI FONDAMENTALI ALLA PRIVACY E PROTEZIONE DATI

- ***Diritto di accesso***: l'interessato può chiedere conferma se i propri dati sono trattati, ottenere una copia e informazioni dettagliate sulle finalità.
- ***Diritto di rettifica***: possibilità di correggere dati inesatti o incompleti.
- ***Diritto alla cancellazione***: l'interessato può richiedere la cancellazione dei dati quando non sono più necessari, se revoca il consenso o se il trattamento è illecito.
- ***Diritto alla limitazione del trattamento***: in alcune situazioni l'interessato può chiedere di sospendere temporaneamente il trattamento dei dati.
- ***Diritto di opposizione***: possibilità di opporsi al trattamento dei dati per motivi legittimi o per finalità di marketing.
- ***Diritto alla portabilità dei dati***: l'interessato può ricevere i propri dati in un formato strutturato e trasmetterli a un altro titolare.
- ***Diritto di revoca del consenso***: l'interessato può ritirare il consenso in qualsiasi momento, interrompendo il trattamento basato su di esso.

BILANCIAMENTO TRA SICUREZZA E PRIVACY

Il bilanciamento tra sicurezza e privacy è un processo fondamentale per garantire che la protezione dei dati personali non venga compromessa dalle esigenze di sicurezza, e viceversa. Nel GDPR, questo bilanciamento si concretizza soprattutto quando il titolare deve valutare e dimostrare che il proprio interesse legittimo prevale sui diritti e le libertà fondamentali dell'interessato.

In sintesi, bilanciare sicurezza e privacy significa adottare misure adeguate che garantiscano la protezione dei dati personali senza ostacolare legittime esigenze di sicurezza.

ASIMMETRIE INFORMATIVE E POTERE DEI DATI

L’asimmetria informativa si verifica quando una parte ha più informazioni di un’altra, creando un vantaggio e potere economico. Nel contesto dei dati personali, chi controlla grandi quantità di informazioni ha un potere significativo, influenzando mercati e comportamenti. Per ridurre questo squilibrio, sono importanti trasparenza, regolamentazione e tutela della privacy, che aiutano a proteggere gli individui e bilanciare il potere dei dati.

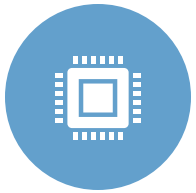
IMPLICAZIONI GLOBALI DELLE NORMATIVE EUROPEE

- Le normative europee sulla protezione dei dati, soprattutto il GDPR, hanno un impatto globale perché stabiliscono standard elevati che influenzano leggi e pratiche in tutto il mondo. Il GDPR regola anche i trasferimenti internazionali di dati, imponendo protezioni anche fuori dall'UE. Ha rafforzato i diritti dei cittadini, aumentato la trasparenza e introdotto sanzioni severe (Fino a 20 milioni di Euro o 4% del fatturato globale annuo), spingendo aziende e governi a migliorare la sicurezza e la privacy.

SOLUZIONI PER LA SICUREZZA DEI PROPRI DATI

Crittografia dei dati: proteggere i dati sensibili rendendoli illeggibili a chi non possiede la chiave di decrittazione.

Gestione dei diritti di accesso: limitare l'accesso ai dati solo al personale autorizzato.

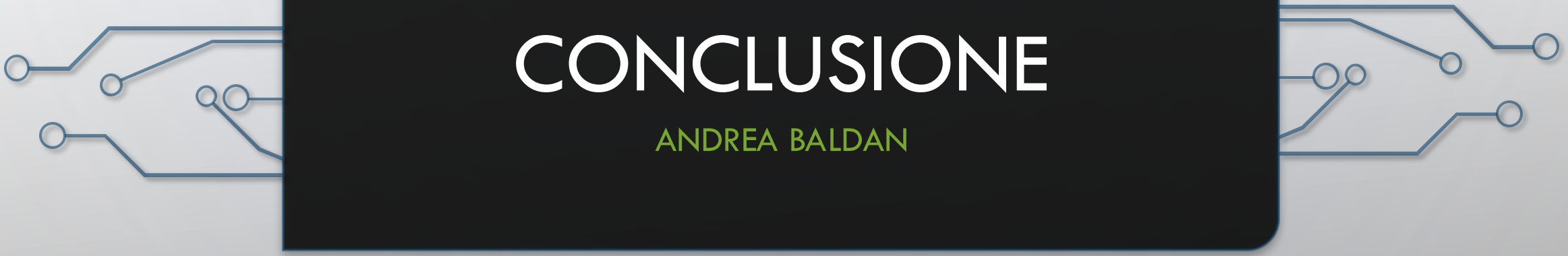


Sicurezza della rete: implementare firewall, sistemi antivirus e anti-malware, monitoraggio del traffico e rilevamento delle anomalie per prevenire accessi non autorizzati e attacchi informatici.

Backup regolari e disaster recovery: effettuare copie di sicurezza dei dati e predisporre piani di recupero.

Autenticazione a più fattori: rafforzare la protezione degli accessi richiedendo, oltre alla password, un secondo fattore di verifica come codici temporanei o dati biometrici.

Conformità al GDPR: adottare misure tecniche e organizzative per rispettare le normative sulla protezione dei dati personali, inclusa la nomina di un Data Protection Officer (garantisce che un'organizzazione rispetti le norme europee in materia di protezione dei dati personali) e la gestione dei data breach.



CONCLUSIONE

ANDREA BALDAN