Informatica

White paper

Consigli su come gestire la "D" del GDPR

INFORMAZIONI SU INFORMATICA

La Digital Transformation cambia le nostre aspettative: servizi migliori, consegne più rapide, il tutto a costi minori. Le aziende devono trasformarsi per restare competitive e i dati sono la risposta per riuscirci.

Quale leader mondiale nell'Enterprise Cloud Data Management, possiamo supportarti per evolvere in modo intelligente in qualsiasi settore, categoria o nicchia di mercato. Informatica ti offre la possibilità di diventare più agile, realizzare nuove opportunità di crescita o persino inventare cose nuove. Siamo focalizzati al 100% sui dati e questo ti offrirà la flessibilità necessaria per competere ed avere successo.

Ti invitiamo a scoprire tutto quello che Informatica ha da offrirti, sprigionando "the power of data" per promuovere la tua prossima intelligent disruption.

Indice

1. Executive summary

Da maggio 2018 entrerà in vigore il Regolamento Generale sulla Protezione dei Dati (GDPR, General Data Protection Regulation) dell'Unione Europea per garantire una maggiore protezione dei dati personali. Il GDPR si applica a tutte le organizzazioni con sede nella UE e a tutte le organizzazioni (in qualsiasi parte del mondo) che elaborano i dati personali degli interessati dell'Unione Europea in caso di offerta di beni o servizi oppure di monitoraggio o tracciamento delle loro attività. Questo regolamento potrebbe avere un notevole impatto per molte organizzazioni e per il loro modo di gestire i dati di clienti, consumatori, partner, personale e altri "interessati", dove per "interessato" si intende una persona. Il GDPR influisce sull'archiviazione, l'elaborazione, l'accesso, il trasferimento e la divulgazione dei record di dati oltre a prevedere alcune sanzioni potenzialmente molto importanti in caso di violazione.

Il GDPR richiederà a molte organizzazioni la piena comprensione di come vengono utilizzate le risorse informative attuali e future al fine di integrare questi nuovi requisiti di privacy dei dati e tutelare il diritto alla riservatezza dei cittadini. Per molti, le conseguenti modifiche alle pratiche di gestione delle informazioni richiederanno un'attenta valutazione delle funzionalità attuali e future relative ai dati. Questo documento analizza come la scomposizione di tali requisiti aiuti a comprendere le sfide legate ai dati e a individuare la strada che le organizzazioni possono seguire in merito alle loro iniziative legate al GDPR.

Per agevolare la comprensione, questo documento analizza alcune delle domande più comuni che le organizzazioni pongono circa il percorso verso il GDPR. Queste sono le domande che definiamo iniziali. Per rendere più semplice rispondere a ogni domanda iniziale, abbiamo stabilito una serie di requisiti di funzionalità che riteniamo importanti e, accanto a ogni funzionalità, abbiamo indicato un caso d'uso tecnologico per mostrare come può essere sviluppata ciascuna funzionalità. La tabella che segue illustra la correlazione tra questi elementi.

Domanda iniziale	Requisito di funzionalità	Caso d'uso tecnologico
Dove risiedono tutti i nostri dati potenzialmente rientranti nel GDPR?	Discovery dei dati sensibili e analisi dei rischi	Rilevamento e protezione
Come vengono utilizzati i nostri dati personali?	Interpretazione delle policy	Data governance di livello enterprise
Come gestiamo i dati dei soggetti interessati?	Gestione dei dati personali	Caso d'uso relativi a data matching e data linking
In che modo proteggiamo i dati e impediamo l'accesso non autorizzato?	Abilitazione di controlli per la sicurezza dei dati	Rilevamento e protezione

Esistono anche casi in cui i requisiti, come ad esempio per il consenso all'acquisizione e alla gestione dei dati, possono comprendere diversi requisiti di funzionalità e casi d'uso tecnologici; le organizzazioni devono quindi avere una comprensione chiara delle potenziali complessità coinvolte.

Malgrado il GDPR ponga molte sfide, offre anche molte opportunità legate all'utilizzo dei dati. Questo documento definisce gli approcci a potenziali casi d'uso e si fonda sulla nostra lunga esperienza in materia di gestione dei dati con l'obiettivo di aiutare le organizzazioni ad affrontare queste sfide e contemporaneamente introdurre funzionalità innovative di data governance, sicurezza e gestione dei dati, per ottenere il massimo dai propri programmi di conformità. Informatica offre soluzioni software integrate e innovative per automatizzare, proteggere e controllare i dati e tali soluzioni sono in grado di fornire rapidamente supporto alle organizzazioni per le iniziative legate al GDPR.

2. Quadro generale

2.1 Quadro generale e potenziali implicazioni

La digitalizzazione della società procede rapidamente e quasi tutte le organizzazioni utilizzano le potenzialità dei dati per migliorare le decisioni aziendali, coinvolgere i clienti e i partner e promuovere processi di business innovativi. La Commissione Europea ha riconosciuto che gran parte dei dati creati, raccolti, elaborati e archiviati è costituita di fatto dai dati personali, che possono svelare molte informazioni sui soggetti interessati della UE.

I regolamenti in materia di protezione dei dati esistenti non hanno necessariamente ridotto le preoccupazioni circa la protezione e la sicurezza dei dati personali. La diversità in materia di regolamenti per la protezione dei dati tra gli stati membri della UE frustra i soggetti interessati, infatti il 90% dichiara di volere gli stessi regolamenti per la protezione dei dati in tutta l'Unione Europea, a prescindere da dove i dati siano archiviati o elaborati.*

Pertanto, il GDPR è stato pensato per proteggere meglio i fondamentali diritti alla privacy dei cittadini nell'era digitale e affrontare i problemi relativi alla diversità di normative in materia di protezione dati.

Da maggio 2018, il GDPR imporrà a molte organizzazioni di gestire e proteggere in modo più efficiente i dati di clienti, cittadini, personale e altri soggetti interessati. Questo regolamento si applica ai soggetti interessati dell'Unione Europea, a prescindere dalla nazionalità o dalla residenza, al fine di garantire norme e regole sulla protezione dei dati personali.

Il GDPR è basato su "regole", ovvero le organizzazioni devono considerare quali sono gli obblighi che potrebbero dovere o non dovere rispettare, considerate le circostanze esclusive del proprio business e l'utilizzo dei dati. Pertanto molte organizzazioni dovranno creare un'interpretazione di tali regole per meglio guidare e indirizzare le proprie iniziative relative al GDPR.

Il GDPR richiederà a molte organizzazioni di comprendere meglio come utilizzano le risorse informative attuali e future al fine di ottemperare a queste nuove regole di privacy dei dati. Tutto ciò avrà un impatto sulle persone, i processi, la tecnologia e le pratiche e le policy di gestione dei dati per molte organizzazioni.

Le violazioni al regolamento potrebbero comportare sanzioni pecuniarie notevoli per molte organizzazioni, a seconda del tipo e della portata della violazione. Potrebbero essere imposte multe fino a 20 milioni di euro o pari al 4% del fatturato mondiale totale, se superiore.

2.2 Chi è impattato dal GDPR?

La conformità al GDPR ha molteplici dimensioni e non è limitata dai confini geografici fisici; le organizzazioni in Nord America, Asia e altri paesi devono rispettarlo se archiviano ed elaborano dati di soggetti interessati che fanno parte dell'Unione Europea. Oggi i dati personali sono gestiti da organizzazioni che commerciano direttamente con i consumatori (B2C), organizzazioni che commerciano con altre organizzazioni (B2B), oltre che da società specializzate nell'elaborazione dati. Le organizzazioni che elaborano i dati di interessati dell'UE dovranno comprendere in modo approfondito i requisiti di conformità, a prescindere da quale sia il paese in cui svolgono le proprie attività o hanno i propri data center.

* http://ec.europa.eu/justice/data-protection/reform/index_en.htm

2.3 Che cosa rende complesso il GDPR dal punto di vista dei dati?

Per molte organizzazioni, esistono sfide specifiche legate ai dati in relazione al GDPR. La conformità al GDPR implica il controllo e la governance dei dati personali ovunque si trovino all'interno di un'organizzazione. Tuttavia, la proliferazione dei dati in tutte le organizzazioni e nei relativi ecosistemi di business può rendere difficile la gestione degli stessi. Trend significativi come un aumento della diversità dei dati e il passaggio al Cloud computing vanno ad aggiungersi alle sfide di sicurezza e gestione dei dati dando vita a un panorama IT fortemente dinamico. Per dimostrare queste sfide, forniamo alcune domande alle quali molte organizzazioni faticano a trovare risposta relativamente al GDPR:

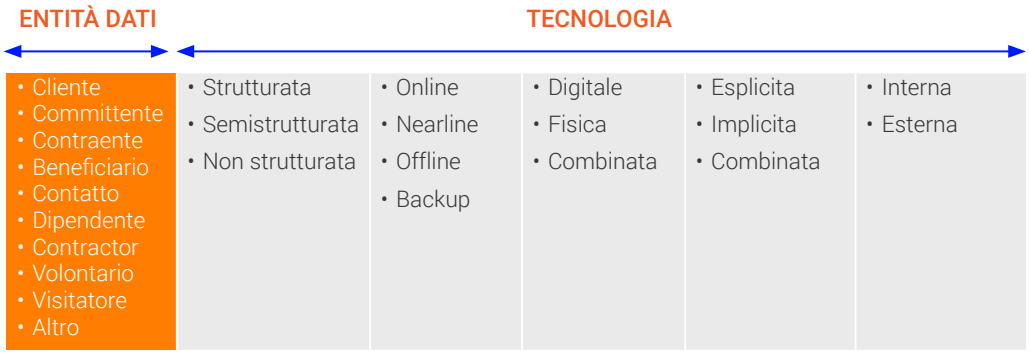
- In un'organizzazione, e nel suo ecosistema, dove si trovano tutti i dati pertinenti ai quali si applicherebbero le regole del GDPR? Tali dati sono a rischio?
- In che modo le organizzazioni tengono traccia dei dati nei propri ecosistemi operativi?
- Come può un'organizzazione definire e gestire tutte le proprie risorse dati pertinenti al fine di garantire che siano applicate e rispettate tutte le necessarie policy e procedure?
- In un'organizzazione dove sono conservati tutti i record di dati ai quali si applicherebbero le regole del GDPR? In che modo possono essere individuati e collegati?
- Come può un'organizzazione acquisire e gestire il consenso fornito da un soggetto interessato? Come può un'organizzazione gestire le modifiche al consenso del soggetto interessato oppure gestire la definizione del consenso?
- Come può un'organizzazione rispondere in modo efficace ed efficiente alle richieste di accesso dei soggetti interessati, al diritto di cancellazione e alle richieste di portabilità entro i termini imposti?
- Come può l'organizzazione controllare l'accesso ai dati pertinenti? I dati riservati vengono rimossi quando non sono necessari per la funzione o l'attività dell'organizzazione?

2.4 Tipi di dati potenzialmente rientranti nel GDPR

Un'altra possibile sfida è come rispondono le organizzazioni ai tipi di dati che conservano. In questo contesto, definiamo due tipi:

1. Tipo di entità dei dati
2. Tipo di tecnologia, che gestisce il tipo di entità dei dati

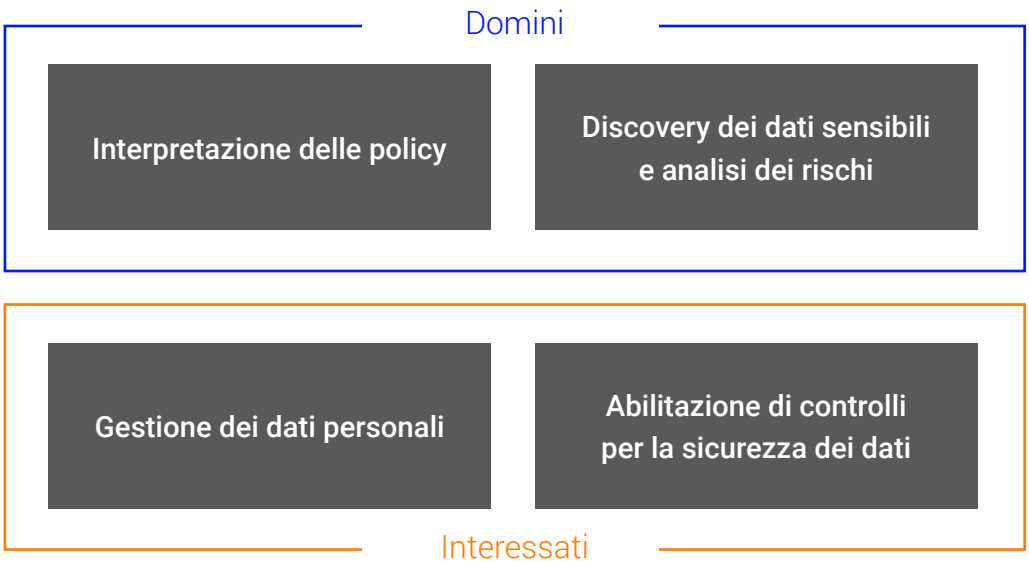
La maggior parte delle informazioni sugli interessati ricade in uno o più tipi di entità dei dati, oltre che in uno o più tipi di tecnologia. Il diagramma seguente illustra alcuni esempi di potenziali tipi di dati e tecnologia che possono essere applicabili ai dati in ambito GDPR:



Questi tipi differenti possono richiedere alle organizzazioni di considerare approcci, metodi e tecnologie molto differenti per l'acquisizione e la gestione delle risorse dati che rientrano nel GDPR.

3. Spunti iniziali, requisiti di funzionalità e casi d'uso tecnologici

Per agevolare la comprensione e la consapevolezza, nonché aiutare nella pianificazione delle attività, Informatica ha individuato una serie di domande iniziali chiave che evidenziano alcune delle sfide legate ai dati in ambito GDPR. Questi spunti iniziali sono spesso guidati da semplici domande che potrebbero portare le organizzazioni a considerare attentamente le persone, la tecnologia e i processi necessari ad ottenere le risposte attese. Per contribuire a rispondere a tali domande abbiamo definito le funzionalità potenzialmente richieste, oltre ad alcuni casi d'uso tecnologiciche garantiscono tali funzionalità. Le funzionalità richieste sono strutturate in due gruppi; il diagramma che segue illustra come funziona tale raggruppamento e la rilevanza di ciascun gruppo.



Le funzionalità rientrano in due aree chiamate domini e soggetti interessati al trattamento dei dati.

Domini rimanda ai domini dei dati dei soggetti interessati. Quest'area aiuta a fornire conoscenze sulla discovery e la gestione dei domini, utilizzate per definire l'ambito e fornire una vista organizzativa dei dati.

Soggetti interessati rimanda ai dati effettivi degli interessati a un livello transazionale. Quest'area aiuta a fornire conoscenze sulla gestione dei dati personali, utilizzata per fornire risposte e un insight dei soggetti interessati..

3.1 Domanda iniziale: Dove risiedono tutti i nostri dati potenzialmente rientranti nel GDPR?
Quadro generale: i dati sono generalmente dispersi tra tutti i diversi sistemi, applicazioni e fonti di un'azienda. Questo vale in particolare per le organizzazioni più grandi e quelle che diventano più grandi in seguito a un'acquisizione. A causa dei ruoli che potrebbero ricoprire i soggetti interessati al trattamento dei dati dell'Unione Europea all'interno di un'organizzazione (cliente, fornitore, partner, dipendente, ecc.), è improbabile che i dati personali siano confinati in un singolo sistema o dipartimento. Le organizzazioni con molti sistemi IT differenti non dovrebbero considerare unicamente i dati nelle applicazioni principali, ma anche quelli di fogli di calcolo, database locali e soluzioni Big Data.

Funzionalità richieste: la discovery dei dati sensibili e l'analisi dei rischi rappresentano una funzionalità che consente di rilevare i dati in una vasta gamma di soluzioni tecnologiche e di utilizzarli, insieme ad altre fonti di informazioni come ad esempio i volumi di dati effettivi e la proliferazione dei dati, al fine di creare un punteggio di rischio per i dati. Il punteggio di rischio consente alle organizzazioni di comprendere dove sono archiviati i dati a rischio più elevato in modo da assegnare la priorità a tutti i potenziali requisiti di correzione o controllo della sicurezza in base a un rischio. Il tracking del punteggio di rischio nel tempo mostra se le attività di correzione o controllo hanno migliorato la posizione di rischio dei dati. A sostegno delle finalità legittime, può essere richiesto il consenso affinché le funzionalità, come ad esempio il lineage dei dati, aiutino le organizzazioni a identificare nuovi store di dati personali per comprendere meglio le potenziali modifiche dell'utilizzo.

Caso d'uso tecnologico: la discovery dei dati sensibili e l'analisi dei rischi potrebbero essere definite come un caso d'uso di rilevamento e protezione, con particolare attenzione alla parte relativa al rilevamento. Si tratta di funzionalità fondamentali per fornire conoscenze su dove risiedono i dati sensibili che rientrano nel GDPR e su dove proliferano, fornendo conoscenze analitiche sui rischi dei dati. Tra le comuni funzionalità che potrebbero valere per questo caso d'uso troviamo:

- **Definizione delle policy dei dati:** definizioni di business e IT, dati vaghi, conflitto di policy
- **Discovery dei dati automatizzata:** ricerca dei dati sensibili rientranti in questo ambito, primo passo più continuo monitoraggio, classificazione dei dati, integrazione dei sistemi di supporto
- **Proliferazione dei dati:** dove sono i dati? Dove vanno? Nuove fonti?
- **Punteggio di rischio dei dati:** basato su spostamento dei dati + proliferazione + accesso + volume, assegnazione priorità più pianificazione, cronologia e monitoraggio del punteggio nel tempo
- **Protezione dei dati:** individuare dove sono necessarie limitazioni all'accesso ai dati, quali dati devono essere pseudonimizzati, dove deve essere applicata la crittografia e visualizzazione dei dati in base a ora, luogo e ruolo

Soluzioni tecnologiche: Informatica Secure@Source può essere utilizzato per agevolare la discovery dell'ubicazione dei dati rientranti in questo ambito, la classificazione dei dati, il monitoraggio della proliferazione dei dati e l'assegnazione dei punteggi di rischio. Il tracking nel tempo mostra come le modifiche influenzino in modo negativo o positivo le iniziative legate alla conformità.

Vantaggio: non solo fornire conoscenze riguardanti l'ubicazione dei dati ma anche classificare i dati in base al rischio.

3.2 Domanda iniziale: Come vengono utilizzati i nostri dati personali?

Quadro generale: il nostro mondo sta vivendo una trasformazione digitale che influisce su tutti i settori. L'aumento dei dati generati, raccolti e analizzati è un chiaro trend mondiale e una percentuale notevole di tali dati può essere costituita da dati personali. Con la proliferazione dei dati in un'organizzazione, l'ownership, il controllo e la gestione di tali dati diventano più complessi. Come molti tipi di conformità alle normative, anche la conformità al GDPR sarà raggiunta in modo ottimale adottando un approccio di livello enterprise alla data governance.

Funzionalità richieste: l'interpretazione delle policy è una funzionalità che consente di acquisire da un punto di vista tanto del business quanto della tecnologia una comprensione di policy, responsabilità, processi, condizioni relative ai dati e modelli logici e fisici. In particolare, è il punto dove la comprensione dell'ambiente tecnico è collegata alla comprensione dell'ambiente di business. Tale collegamento offre alle organizzazioni una vista olistica delle informazioni sui domini dei dati in ambito GDPR e fa parte integrante di un approccio alla gestione delle risorse dati.

Caso d'uso tecnologico: l'interpretazione delle policy potrebbe essere definita come un caso d'uso di data governance di livello enterprise. Si tratta di funzionalità fondamentali per fornire una vista top-down e bottom-up della gestione dei dati nell'organizzazione, con collegamenti tra la vista business e la vista IT delle informazioni. Tra i comuni requisiti che si applicherebbero a questo caso d'uso troviamo:

- **Definizione delle policy:** definizioni di business e IT, documentazione su tutti i livelli operativi del business, modelli di processi e dati fisici e logici
- **Responsabilità:** chi possiede i dati, chi utilizza i dati e quali funzioni sono responsabili della qualità e della sicurezza?
- **Definizione dei termini e dei processi:** processi di business, principali entità dei dati, attributi, sistemi, qualità e controlli, standardizzazione, definizioni di business del consenso
- **Processo di modifica:** processo governato per le definizioni, processo governato per la modifica, governance dei processi
- **Collegamento alle risorse:** collegamento da risorse logiche a fisiche, lineage dei dati di business e tecnici, integrazione della data quality

Soluzioni tecnologiche: adozione di soluzioni di data governance di livello enterprise che consentano alle funzioni business e IT di collaborare per raggiungere l'obiettivo comune della data governance. Soluzioni come ad esempio **Informatica Axon Data Governance** sono progettate appositamente per unire le viste business e IT dei dati e creare collegamenti tra risorse dati logiche e fisiche.

Vantaggio: contributo rapido e semplice da parte di tutti gli esperti in materia per definire i processi, le policy e le entità dei dati che l'organizzazione ha per creare rapidamente una funzionalità di data governance olistica per i dati contemplati nel GDPR.

3.3 Domanda iniziale: Come gestiamo i dati degli interessati?

Quadro generale: come conseguenza diretta dell'utilizzo differenziato dei dati in ambienti IT complessi, creare un'unica vista di tutte le informazioni per i singoli interessati diventa una sfida. Questa sfida deriva dal fatto che diversi sistemi utilizzano meccanismi molto diversi per archiviare e indicizzare i dati. Senza una vista completa dei dati dei singoli soggetti interessati dal trattamento dei dati e di come tali dati sono archiviati, gestiti o elaborati in un'organizzazione, la conformità al GDPR sarà molto difficile da raggiungere, in particolare per quanto concerne i diritti dei singoli interessati.

Funzionalità richieste: la gestione dei dati personali è una funzionalità che consente di individuare i record dei soggetti interessati all'interno di tutte le fonti identificate, di associare e collegare i record per ogni singolo soggetto interessato e di creare un repository Entity 360. Tale repository rappresenta una fonte dati di qualità elevata che indica quali record di dati effettivi sono conservati nelle fonti rientranti in questo ambito e come ciascun dato è collegato a un singolo soggetto interessato. Il repository Entity 360 può fungere da fonte dati autorevole quando le organizzazioni rispondono alle richieste dei soggetti interessati in merito ad accesso, diritto di cancellazione o diritto di portabilità. Dal punto di vista del business, Entity 360 può supportare le organizzazioni nella definizione del consenso per l'uso dei dati personali e successivamente nel gestire il consenso stesso: quando è stato fornito/ritirato, attraverso quale canale e quali condizioni specifiche sono state accettate?

Caso d'uso tecnologico: la gestione dei dati personali può essere definita come un caso d'uso relativo ad associazione e collegamento dei dati. Si tratta di funzionalità fondamentali per individuare i record di dati dei soggetti interessati nei sistemi e fornire una vista inter-sistema dei dati associando i record simili e creando collegamenti. Tra le comuni funzionalità che potrebbero valere per questo caso d'uso troviamo:

- **Accesso ai dati pertinenti:** profilazione dei dati degli interessati, estrazione dei dati pertinenti dai sistemi sorgente, applicazione di processi analitici a contenuti semistrutturati e non strutturati
- **Elaborazione della data quality:** valutazione dei livelli di data quality, applicazione di correzioni manuali/automatiche, controllo dei processi per la correzione manuale, reporting di metriche
- **Unica fonte affidabile di dati sugli interessati che include il consenso, come viene ottenuto e come viene gestito:** sono comprese diverse viste e prospettive sull'interessato in funzione dei consensi espressi
- **Associazione e collegamento:** definizione di regole di associazione in base alle definizioni dei processi di business, associazione di record, collegamento di record simili con punteggio, associazione del consenso
- **Persistenza dei dati:** persistenza di record collegati/non collegati, analytics e report

Soluzioni tecnologiche: adozione di soluzioni che agevolano la discovery dei record degli interessati da tutti i domini dei dati, utilizzando algoritmi avanzati per associare tutti i dati correlati allo stesso interessato, indipendentemente da dove sono archiviati i dati. **Informatica Relate 360** utilizza al meglio gli algoritmi avanzati per identificare i dati associati allo stesso interessato e il Master Data Management fornisce il framework per mantenere e gestire una vista comune dei dati sugli interessati.

Vantaggi: una vista unica degli interessati che ha dimostrato vantaggi di business che vanno al di là del GDPR. Ciò vale in particolare se l'interessato in questione è un cliente, che sempre più si aspetta esperienze personali su misura. Dal punto di vista del GDPR, la possibilità di collegare tutti i dati per ogni singolo soggetto interessato agevola il compito relativo al rispetto dei diritti dell'interessato. Sono inclusi il diritto di comprendere l'utilizzo dei dati, il diritto all'oblio e la garanzia che il consenso sia applicato correttamente.

3.4 Domanda iniziale: In che modo proteggiamo i dati e impediamo l'accesso non autorizzato?
Quadro generale: i controlli sulla protezione dei dati rappresentano un approccio volto all'attuazione dei requisiti di consenso del GDPR e agevolano la protezione dei dati personali. Potrebbe esistere da parte dell'IT il requisito di rimozione, mascheramento o pseudonimizzazione dei dati di produzione utilizzati con finalità di testing o pseudonimizzazione dei dati utilizzati per i trasferimenti di dati esterni. Il controllo dell'accesso ai dati per i dati personali a livello utente nelle applicazioni dovrebbe essere rivisto ai fini della conformità.

Funzionalità richieste: anche il **rilevamento e la protezione** forniscono controlli degli accessi e protezione delle informazioni sui soggetti interessati. Le informazioni sugli interessati spesso sono esposte a molti soggetti diversi in un'organizzazione e nel suo ecosistema. I controlli per la sicurezza dei dati sono utilizzati per rimuovere o nascondere le informazioni sui soggetti interessati al trattamento dei dati a chi non deve avere la possibilità di visualizzarli, rendendo al contempo disponibili le stesse informazioni a chi invece ha necessità di visualizzarle

Caso d'uso tecnologico: abilitare il controllo del consenso può essere definito come caso d'uso di rilevamento e protezione. Si tratta di funzionalità fondamentali per proteggere e rendere sicuro l'accesso ai dati, applicando controlli focalizzati sui dati come ad esempio mascheramento, crittografia e controlli degli accessi, nonché gestire il ciclo di vita dei dati compresa l'archiviazione e la cancellazione dei dati e dell'applicazione. Tra le comuni funzionalità che potrebbero valere per questo caso d'uso troviamo:

- **Input dall'analisi dei rischi:** utilizzo del punteggio di rischio per gestire i metodi di controllo dei dati
- **Orchestrazione:** capacità di programmare e coordinare le attività di protezione dei dati in base ai rischi individuati e monitoraggio delle condizioni o degli accessi non sicuri
- **Controlli per la sicurezza dei dati:** mascheramento statico o dinamico, pseudonimizzazione, accesso basato su ruoli, crittografia o tokenizzazione.
- **Cronologia modifiche/aggiornamenti:** applicazione sui sistemi sorgente, mascheramento dei record o risultati dell'archiviazione rispetto al record del consenso, generazione di audit trail come prova
- **Archiviazione:** archiviazione dei dati al di fuori dei sistemi di produzione, attività di log per fornire prove, spostamento offline per evitare l'utilizzo o l'accesso accidentali

Soluzioni tecnologiche: adozione di soluzioni che possano agevolare la gestione del ciclo di vita delle risorse dati e applicazione di controlli su tali risorse. **Informatica Persistent Data Masking** e **Informatica Dynamic Data Masking** possono essere utilizzati per rendere più semplice limitare il numero di persone e sistemi che hanno accesso non limitato ai dati personali. **Informatica Secure@Source** garantisce il ripristino della sicurezza dei dati orchestrando gli aggiornamenti ai controlli di sicurezza.

Vantaggi: introduzione dell'automazione nel data masking per ridurre il rischio di violazioni dei dati personali. La visibilità dei dati personali è limitata agli utenti autorizzati e i dati personali non vengono sottoposti a proliferazione senza il livello adeguato di protezione.

4. Partner

Come spesso accade per le normative e la conformità, quest'ultima non può essere garantita solo dalla tecnologia. Le organizzazioni possono avere bisogno dei migliori esperti e di leader per il proprio percorso per adempiere al GDPR, oltre che di soluzioni tecnologiche e servizi tradizionali. Informatica collabora con molti partner altamente qualificati e competenti per supportarti nella tua iniziativa relativa al GDPR. Tali partner sono stati appositamente selezionati per la loro profonda conoscenza e expertise nella gestione dei dati e l'attenzione alla conformità al GDPR.

Trova il partner giusto per te oppure contatta il rappresentante Informatica di zona, che potrà aiutarti a individuare il partner più adatto in base alle tue esigenze e ai tuoi requisiti.

5. Conclusione

Questo documento evidenzia la necessità per le organizzazioni di considerare le implicazioni in materia di dati imposte dal GDPR. Il nuovo regolamento porta con sé sia sfide che opportunità per molte organizzazioni. Considerato il breve periodo che ci separa dall'entrata in vigore del regolamento, molte organizzazioni dovranno considerare come la propria interpretazione delle regole del GDPR influirà sui processi di gestione dei dati attuali e futuri.

Per aiutare le organizzazioni a iniziare rapidamente a rendere operative tali interpretazioni, Informatica ha individuato una serie di domande iniziali chiave che gli stakeholder pongono e ha suggerito alcune funzionalità che saranno necessarie per rispondere a tali domande. Le domande e le funzionalità non affrontano solo una parte della serie di requisiti del GDPR, ma aiutano a creare un insieme completo di funzionalità per affrontare molte delle sfide legate ai dati che il GDPR comporta.

Accanto a ogni funzionalità troviamo un caso d'uso tecnologico. Ogni caso d'uso definisce i tipi di soluzioni software e le tecnologie che potrebbero essere utilizzati per portarlo a termine.

Informatica è il vendor leader nel settore per le soluzioni di data management da oltre 20 anni e ha risolto sfide complesse legate alla gestione dei dati per migliaia di organizzazioni in tutto il mondo. Il GDPR implicherà molte sfide complesse in termini di gestione dei dati per molte organizzazioni. Informatica e l'ecosistema dei suoi partner sono nella posizione ideale per aiutare tali organizzazioni con le loro iniziative legate al GDPR.

6. Dichiarazione di limitazione di responsabilità

La conformità al GDPR si baserà su fattori specifici legati al business, all'attività e all'utilizzo dei dati da parte di un'organizzazione. Questo documento fornisce una serie di punti di discussione che potrebbero essere utili nel percorso compiuto da un'organizzazione verso la conformità al GDPR e non sono destinati a fornire consulenza legale, indicazioni o consigli. Per ottenere informazioni sugli obblighi da adempiere, è necessario rivolgersi al proprio consulente legale.

Informatica

Informatica Software Italia srl, Piazza della Repubblica 14/16 - 20124 Milano Telefono: +39 02 37 05 80 00 IN09_0218_03337
www.informatica.com/it www.informatica.com linkedin.com/company/informatica twitter.com/InformaticaITA