Panoramica sulla conformità di Arca Cloud GDPR

General Data Protection Regulation

Kit di conformita

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

12 passaggi alla conformità GDPR

Il 25 maggio 2018 il regolamento generale sulla protezione dei dati (GDPR) (regolamento (UE) 2016/679) è diventato esecutivo. Questo regolamento intende rafforzare e unificare la protezione dei dati per tutti gli individui all'interno del Unione Europea (UE),viene applicato a tutte le entità che trattano i dati personali di Cittadini dell'UE.

La legge crea complicazioni per le organizzazioni che si occupano di dati di privati cittadini, soprattutto quando è condivisa oltre i confini dell'organizzazione. La conformità è semplificata quando i dati vengono ,assegnati a terze parti(professionisti) o ad applicazioni(Self-Hosted) che interfacciano il titolare dei dati e il titolare del trattamento .Il self-hosting Arca-cloud è uno dei modi più facili per garantire conformità con la GDPR e leggi simili in tutto il mondo.

Obiettivi di questo documento In questo documento, ti proponiamo una panoramica di base dei passaggi da adottare ,per qualsiasi organizzazione al fine di essere conformi a GDPR. Si prega di essere consapevoli del fatto che questo non è in alcun modo un consiglio legale. Se non sei sicuro di essere Conforme alla GDPR in ArcaCloud, si prega di mettersi in contatto con noi attraverso le informazioni di contattato mensionate sopra il documento, e faremo del nostro meglio per chiarire ogni dubbio, insieme ai nostri rappresentati legali .

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

1 / Siate consapevoli delle modifiche necessarie

Prima di tutto, dovresti identificare le aree della tua organizzazione e ciò potrebbe causare problemi di conformità.

Un modo per farlo è, se ne hai uno, consultare il registro dei rischi. Se la tua organizzazione è di grandi dimensioni, non dimenticarti che avrai bisogno di tempo ed energie , tutti elementi da non sottovalutare.

Oramai,dovresti già aver appreso i 12 passaggi descritti in questa guida - se non l'hai fatto, inizia adesso e considera questo come un processo di fondamentale importanza ! tutti devono essere conformi entro il 25 maggio 2018. Un ritardo nel completamento di questo passaggo chiave significa che non sarai conforme in tempo e rischi un ammenda pari a 20 milioni di euro, o il 4% del tuo fatturato globale annuo .

Inoltre, dovresti assicurarti che tutto il personale e le figure di riferimento della tua organizzazione siano a conoscenza dei cambiamenti di legge che avvengono con la GDPR al fine di assicurarsi che nessuna decisione possa infrangere La legge . La GDPR viene applicata all’interno della tua organizzazione diventando conforme applicando cambiamenti futuri nel modo in cui il tua azienda detiene dati appartenenti a terzi .

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

2 / Diventate consapevoli delle informazioni in vostro possesso

In questa seconda fase, è essenziale documentare chi saranno le persone chiave e le figure all'interno della tua azienda che saranno responsabili dei dati e capire la tipologia di dati di cui siamo in possesso . Nel caso in cui non sarai in grado di essere conforme e non si è a conoscenza di quali informazioni si detengono e la GDPR richiede di documentare, dimostrare e registrare in che modo la tua organizzazione è conforme. Ecco le domande che dovresti porti sulla documentazione:

- Perché stai tenendo i dati?
- Perché hai raccolto i dati?
- Come hai ottenuto i dati?
- Per quanto tempo conserverai i dati?
- Con quale sicurezza stai conservando i dati? Come vengono crittografati? Chi può accedervi?
- Condivi questi dati con terze parti? Su quali stai condividendo i dati con quelle terze parti?

Mentre è possibile raggiungere questo obiettivo in un modo piuttosto semplice per le piccole organizzazioni.
Se invece la tua organizzazione è grande, puoi tranquillamente farlo pero' è necessario un controllo delle informazioni per ottenere una conoscenza sufficiente sui dati che detieni.
La documentazione diventa ancora più importante se viene condivisa con terze parti .
A tal punto sarà necessario essere in grado di notificare qualsiasi organizzazione con cui condividi i dati , nella situazione in cui scoprissi che tale condivisione è inaccurata e mette a repentaglio la loro sicurezza.

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

3 / Comunicare le informazioni sulla privacy con il personale e gli utenti.

Per essere conforme, è necessario rivedere i dati correnti e gli avvisi sulla privacy che avvisano il personale e / o gli utenti riguardo la raccolta dei loro dati. Identifica tutti quegli elementi che non informano gli utenti sui loro dati in uso ed eliminali . Secondo la legge vigente, le informative sulla privacy devono informare gli utenti (titolare dei dati) su :

- la tua identità
- i motivi per cui raccogli i loro dati
- che uso fai dei loro dati
- a chi sarà reso noto -
- se i dati saranno trasferiti al di fuori dell'UE.

Con la GDPR, devi inoltre informarli :

- la base legale per il trattamento dei dati che raccogli
- quali periodi di conservazione si applicano
- se i dati dei tuoi utenti saranno sottoposti ad automatizzazione
- il fatto che i tuoi utenti abbiano il diritto al reclamo, se sono
- insoddisfatti del modo in cui si implementa uno di questi criteri
- in generale, i loro diritti individuali ai sensi della GDPR.

La GDPR richiede anche che tu ti assicuri che tali avvisi siano Concisi e facili da capire per tutti - prova a usare facilmente la lingua ed evitare qualsiasi uso di termini tecnici o legali.

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

4 / Assicurati che le tue procedure coprano tutti i diritti sulla privacy personale

Dovresti conoscere tutti i diritti che la GDPR concede ai singoli e adottare misure per rispettare tali diritti. Questi sono i diritti garantiti dal GDPR:

- il diritto di essere informato su quali dati si conservano e come essere elaborati
- il diritto di accedere ai dati conservati dalla tua organizzazione
- il diritto di rettifica dei dati memorizzati
- il diritto alla cancellazione dei propri dati personali
- il diritto di limitare l'elaborazione; dei propri dati personali
- il diritto di opporsi alla conservazione o all'elaborazione dei dati
- il diritto di non essere soggetti a decisioni automatizzate, compresa la profilazione
- il diritto alla portabilità dei dati.

Si noti che il diritto alla portabilità dei dati è nuovo e si applica solo in tre casi specifici:
dati personali forniti da una persona a un controllore
nei casi in cui l'elaborazione è basata per l'esecuzione di a contratto o sul consenso della persona
se il trattamento è effettuato con mezzi automatizzati.

È essenziale che la tua organizzazione consideri se le tue procedure applicate rispettino questi diritti e se è necessario effettuare modifiche per essere conforme a GDPR.

Assicurati che tutti questi diritti siano rispettati. Include capire in anticipo come vengono cancellati i dati personali e poter informare utenti o personale del modo in cui questo è avvenuto, in modo da evitare sanzioni. Include anche capire in anticipo in che modo fornirai i dati personali elettronicamente in casi in cui i tuoi utenti lo chiedono; devi essere in grado di fornire questi dati in un formato comunemente usato.

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

5 / Essere in grado di gestire le richieste di accesso

Il GDPR apporta cambiamenti nel modo in cui la tua organizzazione deve confrontare le richieste di accesso del soggetto.
Per essere conforme, dovresti rivedere e aggiornare le procedure attuali per gestire tutte le richieste di accesso.

Dovresti essere consapevole delle nuove tempistiche: mentre al momento hai 40 giorni per conformarsi alle richieste di accesso, ai sensi della GDPR questo il tempo sarà ridotto a un mese. Il GDPR richiede che tu dia agli individui la richiesta di accesso a informazioni aggiuntive come i periodi di conservazione dei dati applicati dalla propria organizzazione e il loro diritto di rettificare i dati che si ritengono siano imprecisi. Generalmente non ti è permesso addebitare nessun costo per il rispetto di tale richiesta.

Tuttavia puoi rifiutare o addebitare una richiesta di accesso se riesci a dimostrare che il costo per la tua organizzazione sarà eccessivo, o se la richiesta manifestata è infondata. Se rifiuti una richiesta, dovrai comunicare chiaramente il tuo rifiuto, e informare la persona delle ragioni per questo rifiuto. Inoltre, dovrai farlo informando la persona del suo diritto di presentare reclamo alla vigilanza .

Un autorità in carica troverà un rimedio giurisdizionale. I rifiuti devono essere comunicati entro un mese non più tardi. Se la tua organizzazione gestisce una grande quantità di richieste di accesso, devi essere preparato ad affrontare l'impatto di questi cambiamenti.

Fornire informazioni aggiuntive e trattare le richieste in tempi più brevi costeranno alla tua organizzazione molto tempo. Se puoi prendi in considerazione lo sviluppo di sistemi automatizzati facendo accedere le persone alle loro informazioni online .

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

6 / Conoscere le basi legali per l'elaborazione dei dati personali.

Hai pensato alle basi legali della tua organizzazione per elaborare dati personali?
In caso contrario, dovresti farlo per essere Conforme alla GDPR.
È essenziale esaminare i vari tipi di dati trasportati fuori dalla tua organizzazione.

La base legale per l'elaborazione dei dati è generalmente la stessa prima e dopo la GDPR. Tuttavia, le implicazioni pratiche sono modificate dalla GDPR come i diritti individuali sono modificati in base alla base legale per l'elaborazione dei loro dati.
Anche questo deve essere affrontato nella tua informativa sulla privacy: è necessario spiegare la base giuridica per l'elaborazione dei dati dell'utente. Inoltre, dovrai menzionarla quando rispondi a richiesta di accesso per ogni singolo soggetto.

Quando non esiste una base giuridica specifica per l'elaborazione personale dati, dovrai fare affidamento sul consenso come base legale.

Questo significa che gli individui avranno un diritto più forte di cancellare i propri dati o modificarli, in quanto il consenso può essere ritirato.
Se possibile, riduci la quantità di tipi di dati che mantieni, come ogni tipo di dati che raccogli dovrà essere giustificabile.

Dovresti considerare l'anonimizzazione e / o la pseudonimizzazione di qualsiasi tipo di dati visto che non è necessario archiviare in formato raw.

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

7/ Assicurati di ottenere il consenso per l'elaborazione Dati.

Se la base giuridica su cui si basa il trattamento dei dati personali è il consenso,dovresti assicurarti che il modo in cui ottieni il consenso segua lo standard GDPR.
Rivedi come cerchi, gestisci e registri il consenso e applica i cambiamenti necessari Secondo la GDPR, il consenso deve essere liberamente dato, ed essere specifico, informato e non ambiguo.
Ciò significa che:

-Gli utenti non possono essere forzati al consenso.
- Gli utenti devono essere consapevoli di ciò che acconsentono in termini di dati in lavorazione.
- Silenzio e inattività non significano consenso esplicito.
- Le caselle pre-barrate non sono sufficienti per esprimere il consenso esplicito.
- Il consenso deve essere verificabile.
- Le persone devono essere informate del loro diritto di ritirare il consenso che hanno precedentemente espresso e in grado di farlo in a modo semplice.
- Ottenere il consenso dovrebbe avvenire in un modo separato da altri termini e condizioni.

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

8 / Prestare particolare attenzione durante l'elaborazione dati dei bambini

La tua organizzazione è in grado di elaborare i dati dei bambini? In questo caso, dovresti mettere in atto dei sistemi per verificare l'età dell'utente, e ottenere il consenso dei genitori per elaborare i dati di soggetti minorenni .

Il GDPR introdurrà protezioni specifiche per i dati personali dei bambini, in particolare nel contesto del social network e servizi internet commerciali.
Con la GDPR, i bambini saranno in grado di dare il proprio consenso al trattamento dei dati ad anni 16, ma in alcuni stati europei può cambiare questo limite di età, quindi assicurati di conoscere i limiti di età chesi applicano al paese in cui operi.
Sotto questa età, dovrai farlo per ottenere il consenso da una persona in possesso della potestà genitoriale :
- un genitore o un tutore legale.

Anche qui, il consenso deve essere verificabile. Questo significa che tutte le regole impostate nella fase 7 di questa guida devono essere seguite, insieme a un avviso in una lingua che il soggetto minorenne può capire.

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

9 / Sapere come gestire le violazioni dei dati

Quando si tratta di affrontare il rischio di una violazione dei dati che coinvolge dati personali, le procedure corrette devono essere messe in atto da la tua organizzazione entro il 25 maggio 2018.

Con l'entrata in vigore di tale legge Capire come affrontare una violazione dei dati quando accade è troppo tardi. Le procedure per gestire una violazione dei dati comportano il rilevamento di essa, segnalandolo e indagando sul fatto avvenuto.

Secondo la GDPR, le notifiche di violazione saranno obbligatorie per tutte le organizzazioni.
Non tutti i tipi di violazioni dei dati devono essere segnalati: è il caso in cui le violazioni possono causare danni al diritto e alla libertà di persone e causare un significativo impatto sociale o svantaggio economico per qualsiasi individuo i cui dati vengono conservati.

Ad esempio, si tratta di violazioni che potrebbero risultare finanziarie Come perdita di denaro, danno alla reputazione, ecc.

Tali violazioni dei dati devono essere segnalate al responsabile dell'informazione; responsabile nel paese in cui operate. Assicuratevi di essere a conoscenza dei passi da seguire per farlo localmente .

La mancata segnalazione di violazioni dei dati può comportare multe: è essenziale istituire una procedura per reagire tempestivamente.

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

10 / Ulteriori informazioni dell'impatto sulla protezione dei dati con Valutazioni (DPIA) e disegno sulla protezione dei dati .

TLa GDPR introduce la privacy obbligatoria per la progettazione dei dati, la Protezione, e il design sono di default nella legge. In breve: Rendi l'impostazione dei tuoi servizi il più adatta alla privacy possibile. La GDPR effettua anche valutazioni dell'impatto sulla protezione dei dati DPIA - obbligatorio in circostanze specifiche:

- con l'implementazione di una nuova tecnologia
- quando speciali categorie di dati vengono elaborate su larga scala
- con operazioni di profilazione che possono influire sulla privacy di individui.

Quando si effettua una DPIA, la propria organizzazione valuta sistematicamente il potenziale impatto che il vostro trattamento dei dati potrebbe avere sulla privacy delle persone i cui dati vengono conservati, per ogni separato progetto della tua organizzazione.
Facendo una DPIA la tua organizzazione sarà in grado di sapere se le operazioni di elaborazione effettuate dalla tua azienda sono conformi alla GDPR.
Se devi condurre una DPIA per un progetto specifico, le domande che dovresti porti:

-Chi sarà responsabile del progetto?
- Chi altro sarà coinvolto?
- Il processo verrà eseguito centralmente o localmente?

Se scopri dopo una DPIA che la tua organizzazione potrebbe non essere in grado di rispettare il GDPR con piena certezza,

lo è l' obbligo di notificare e consultare le autorità incaricate nell medesimo processo a rischio.

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

11 / Considerare la designazione di una protezione dei dati ufficiale

Non tutte le organizzazioni devono designare un responsabile della protezione dei dati con GDPR. È, tuttavia, essenziale scoprire se avere un responsabile della protezione dei dati è obbligatorio per la vostra organizzazione.

Se la tua organizzazione è un'autorità pubblica, se la tua organizzazione porta con sé il monitoraggio regolare e sistematico di individui di grandi dimensioni o se le organizzazioni elaborano dati sensibili (salute r, informazioni sulla condanna penale, ecc.) su grande scala, dovrai designare un responsabile della protezione dei dati. Il ruolo del responsabile della protezione è quello di assumersi la responsabilità dei tuoi dati e rispettarne la conformità alla protezione, in base alla sua conoscenza dell'argomento, per svolgere questo ruolo fornendo supporto e autorita'; questo ruolo puo' essere svolto da una persona esterna o interna alla tua governance .

12 / Conoscere le regole riguardanti l'elaborazione transfrontaliera.

Questo ultimo passaggio è rilevante solo se la tua organizzazione opera in più di uno stato UE. In questo caso, dovresti determinare
qual è la vostra autorità di controllo principale per la protezione dei dati e documentarlo: LSA è il supervisore nello stato in cui ti trovi che fa capo all'amministrazione centrale all'interno della UE .

C-Planet IT Solutions LTD.
24 Telemetry House,
Conservatory Street,
Floriana, Malta

Malta : +(356) 21 472 196
Italy : (+39) 393 307-63-59

support@arcanet.com.mt
accounts@arcanet.com.mt

Conclusione

La GDPR è un atto legislativo complicato pensato per combinare un patchwork delle norme locali in un'unica legge definitiva sulla protezione dei consumatori. Proteggere la privacy degli utenti, costringendo le organizzazioni a revisionare le loro politiche e il modo in cui vengono gestiti i dati.

ArcaCloud è uno dei modi più semplici per garantire la conformità con la GDPR e leggi simili in tutto il mondo. Se tuttavia si sceglie di avere ArcaCloud come soluzione cloud, hai la possibilita' di avere accesso ai dati da qualunque luogo tu sia. Considera la possibilità di nominare ArcaNet come tuo Responsabile della protezione dei dati per assicurarti di diventare e rimanere in regola.