



# monit<sup>or</sup>ora

## data protection

Pacchetto di soluzioni studiate per garantire la conformità al GDPR, il Regolamento Europeo 2016/679 per la protezione dei dati e della privacy.

Sta per diventare obbligatorio, sia per gli enti pubblici che privati, il **GDPR**, il Regolamento UE 2016/679 con il quale la Commissione Europea intende rafforzare e omogeneizzare la protezione dei dati dei cittadini dell'Unione Europea. Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016, inizierà ad avere efficacia il **25 maggio 2018**.

Non si tratta di un semplice aggiornamento della normativa sulla Privacy: il GDPR tiene conto della necessità di preservare l'integrità del dato e proteggerlo da usi impropri. Perciò le organizzazioni dovranno dotarsi di un insieme di strumenti e servizi che facilitino l'esecuzione delle incombenze richieste dalla norma.

Webgenesys, al fine di supportare i propri clienti nell'approccio e la gestione di quanto necessario per assolvere all'obbligo normativo, propone una soluzione in grado di rispondere alle esigenze di clienti di varie dimensioni sia del settore pubblico che privato.

In caso di inosservanza di quanto previsto dal GDPR, l'Autorità Garante per la Protezione dei Dati Personali potrà imporre di sanzioni di due tipi, sanzioni correttive e sanzioni di carattere economico.

Le sanzioni correttive consistranno in avvertimenti, ammonimenti, richieste di rettifica e, in generale, osservazioni dirette al titolare del trattamento o al responsabile del trattamento.

Le sanzioni di carattere economico, invece, riguarderanno:

- Inosservanza degli obblighi del titolare e del responsabile del trattamento; inosservanza degli obblighi dell'organismo di certificazione; inosservanza degli obblighi dell'organismo di controllo: **fino a 10 milioni di Euro o, per le imprese, fino al 2% del fatturato annuo.**

- Inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati; inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali; inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo: **fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato annuo.**







- Inosservanza di un ordine correttivo dell'Autorità di Controllo: **fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato annuo.**

L'insieme delle soluzioni e dei servizi proposti fa parte del listino **Monitora** ed è distribuito in pacchetti variabili in base alle risorse attive presso ogni cliente:

Data Protection - Micro	Data Protection - Small	Data Protection - Medium	Data Protection - Large
fino a 20 dipendenti	da 21 a 50 dipendenti	da 51 a 100 dipendenti	da 101 a 200 dipendenti
1 giornata di Assessment	2 giornate di Assessment	4 giornate di Assessment	6 giornate di Assessment

Per le organizzazioni con un numero di dipendenti superiore alle 200 unità sarà necessario effettuare un pre-assessment e quotare singolarmente i progetti in base alla complessità organizzativa e alla criticità dei processi in uso.





L'insieme di soluzioni proposte è composto da:

<b>Gestionale GDPR</b> 	<b>Cruscotto direzionale di rete</b> 	<b>Log Management</b> 
<b>Vulnerability Assessment</b> 	<b>Risk Assessment</b> 	<b>Formazione</b> 



Il Gestionale GDPR è sviluppato con il supporto di un team di esperti legali tra i più affermati in Italia e contiene strumenti operativi specifici per rendere rapide e intuitive le attività di adeguamento alla nuova norma GDPR.







Il pannello di gestione del software ha le seguenti caratteristiche:

-  **Web Based:** nessuna installazione richiesta in locale, si utilizza da qualsiasi Sistema Operativo e Browser Web
-  **Completo:** include già tutte le attività di adempimento indicate dal Regolamento Privacy Europeo
-  **Aggiornato:** il software viene continuamente aggiornato da parte del Team di sviluppo con nuove funzionalità e costantemente adeguato alle normative vigenti
-  **Rapido:** il software include tutti gli strumenti che rendono semplice, veloce e intuitiva l'attività di inserimento e aggiornamento dati.

## Cruscotto direzionale di rete



Le funzionalità del Cruscotto sono indispensabili per monitorare lo stato del network, presupposto fondamentale per intervenire tempestivamente e garantire l'integrità del dato e la protezione dello stesso da trafugamento e divulgazione a seguito di intrusione. La soluzione è cloud oriented e si compone di moduli interoperabili e progettati secondo logiche di tipo SaaS che rendono la piattaforma completa sotto il profilo dei servizi:




-  **Asset Management:** consente di inventariare tutti i beni informatici del network
-  **Monitoring stato di rete:** esegue la diagnostica costante della rete e verifica lo stato dei sistemi operativi
-  **Networking:** permette di intervenire tempestivamente su guasti o malfunzionamenti
-  **Ced:** riceve informazioni dai sensori posizionati in sala CED e può prevedere l'automatizzazione delle attività al verificarsi di determinati eventi.
-  **Back Up:** consente il salvataggio dei dati direttamente dalle cartelle appositamente selezionate
-  **Security:** permette l'implementazione delle regole per la gestione della sicurezza della rete



La procedura di inserimento e aggiornamento dei dati è facilitata dalla semplicità d'uso del gestionale GDPR, ideato appositamente per essere utilizzato anche da chi non possiede particolari competenze informatiche.

Tuttavia, gli amministratori di sistema e il personale autorizzato al trattamento dei dati possono incorrere in errori nel caricamento dei dati.

Il sistema di Log Management consente di:

-  tracciare gli accessi di tutti gli utenti ai sistemi e ai dati
-  verificare le modifiche effettuate dagli utenti e il canale di accesso utilizzato (indirizzo IP, geo localizzazione, nome della stazione, etc)
-  verificare le operazioni effettuate dagli utenti nella directory delle identità (Active Directory, etc).

In sostanza, il sistema di Log Management consente di monitorare l'accesso ai dati e alle funzioni di gestione e, correttamente utilizzati, permettono di identificare la persona che compia una delle azioni oggetto del controllo.



Tra le attività fondamentali nella gestione delle attività che consentono il rispetto del GDPR c'è il Vulnerability Assessment, che consiste nell'esecuzione di scansioni automatizzate e semi-automatizzate della rete del cliente.

- 🔍 Le scansioni sono non invasive e sono condotte grazie ad appositi strumenti software.
- 🔍 L'output dell'attività è la rilevazione di vulnerabilità all'interno dell'infrastruttura informatica oggetto di analisi.




L'isolamento tempestivo delle reali vulnerabilità presenti sul perimetro della rete pubblica, o all'interno della rete privata, consentirà al Cliente di mantenere una visione aggiornata del grado di robustezza dei propri sistemi informativi, ottimizzando gli sforzi di gestione della sicurezza.





Oltre agli strumenti software fondamentali per la gestione della sicurezza dei dati, mettiamo a disposizione dei clienti anche l'attività di consulenza mirata a effettuare la mappatura dei principali processi/unità organizzative/dati trattati e alla elaborazione di un Risk Assessment.

Il servizio comprende anche l'elaborazione delle linee guida per il conseguimento/mantenimento della compliance al GDPR, attraverso:




-  interviste finalizzate non solo alla mappatura dei processi standard ed alla individuazione dei rischi ma anche alla compliance con riferimento sia ai diritti dell'interessato (artt 12-22), sia alla responsabilità del titolare del trattamento (artt 24, 26, 28, 29), sia alla liceità del trattamento (artt 6-10), sia alla protezione dei dati. Si sottolinea in particolare che le maggiori sanzioni (fino a 20 milioni di euro ed al 4% del fatturato globale) previste all'art 83 del GDPR sono relative alla violazione degli artt 5, 6, 7, 9 e da 12-22.
-  elaborazioni di possibili misure di contenimento dei rischi individuati
-  l'assessment annuale di rischi e misure di contenimento.



L'art 29 del GDPR prevede un divieto di trattamento del dato per personale che non sia stato istruito dal titolare del trattamento o dal responsabile del trattamento.

Per questo motivo abbiamo predisposto un servizio di consulenza che prevede sessioni formative sui temi della privacy, svolte da esperti del settore ed erogate in modalità e-learning, replicabili on demand e corredate da test di verifica.

Per dare adeguato adempimento a quest'obbligo (l'inadempimento è sanzionato fino a 10milioni di euro e fino al 2% del fatturato globale) si prevedono:

-  attività formativa di carattere generale somministrata in modalità e-learning
-  attività formativa sugli strumenti adottati dall'ente (codice di comportamento, codice etico, regolamenti di accesso, etc) finalizzata ad istruire il personale addetto al trattamento
-  la formazione sarà ripetuta annualmente per dare risposta a modifiche legislative, organizzative e di regolamentazione interna.