ORIGINALE

COMUNE DI SCICLI

(Libero Consorzio Comunale di Ragusa)

Settore I Amministrativo
Servizio CED

DETERMINAZIONE N. 90 DEL 25/05/2018

REGISTRO GENERALE N. 538 DEL 25/05/2018

Oggetto: Affidamento dei servizi per l'adeguamento del sistema di gestione della privacy del comune alle disposizioni del nuovo regolamento europeo 2016/679 sul trattamento dei dati e contestuale incarico per RDP. Determina affidamento e impegno spesa. CIG: Z3C23BFB9C.

IL CAPO SETTORE

Premesso che :
- a partire dal 25/05/2018 sarà direttamente applicabile in tutti gli Stati dell'Unione europea il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- tra le novità introdotte dal Regolamento per gli enti e per le imprese vi sono:
  - l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati;
  - la responsabilizzazione (accountability) dei titolari e dei responsabili del trattamento;
  - l'introduzione della figura del «Responsabile della protezione dei dati» (Data Protection Officer o DPO), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti;

Dato atto che è necessario adeguare il sistema di gestione della privacy del Comune alle disposizioni del nuovo regolamento Europeo sul trattamento dei dati e procedere alla contestuale individuazione del DPO;

Vista la direttiva sindacale n. 34 del 24.05.2018, protocollo generale n. 16375 di pari data, in merito alla attuazione degli adempimenti in materia di privacy di cui al Regolamento Europeo UE 679/2016 (25 maggio 2018) – Designazione RDP/DPO esterno con la quale viene dato mandato alla scrivente di procedere all'affidamento di apposito appalto di servizio di assistenza tecnico giuridica e soluzione software a supporto per l'attuazione del nuovo regolamento europeo 2016/679/UE in materia di privacy e servizio di nomina DPO per l'attuazione del nuovo regolamento europeo;

Dato atto che:
- in esecuzione della suddetta direttiva con determina n. 89 del 25.05.2018 R.G. N° 537 del 25/05/2018 è stata approvata la lettera d'invito da inviare all'unico operatore economico iscritto nell'albo dei fornitori dell'Ente per la categoria B23 "Assistenza e aggiornamento hardware e software;
- con lettera prot. 16504 del 25.05.2018 è stata invitata l'impresa Scalone Giorgio a presentare offerta;
- con nota prot. 16507 del 25.05.2018 sig. Giorgio Scalone, Amministratore Unico dell'Impresa individuale Scalone Giorgio con sede in Ragusa, via A. De Gasperi n. 26, partita IVA 01490400882 ha presentato l'offerta per servizio per l'adeguamento del sistema di gestione della privacy del Comune di Scicli alle disposizioni del nuovo Regolamento Europeo 2016/679 sul trattamento dei dati e contestuale incarico per RDP, per un importo complessivo di € 5.000,00 oltre IVA 22%, pari a € 6.100,00 IVA 22% compresa;

Ritenuto necessario procedere urgentemente alla individuazione del Responsabile della Protezione dei Dati di cui all'art. 37 RGDP, al fine di evitare che l'Ente possa incorrere in responsabilità e sanzioni scaturenti dalla non applicazione del Regolamento stesso;

Ritenuto, nella fattispecie in esame, di applicare l'art. 36, comma 2, lettera a) del d.lgs. 50/2016, che prevede la facoltà di procedere all'affidamento diretto, anche senza previa consultazione di due o più operatori economici nei casi di affidamenti di importi inferiori a € 40.000,00;

Dato atto che questo Ente, con determina n. 34 del 04/05/2018 – R.G. n. 450 di pari data, del Capo Settore IV Gare Contratti Anticorruzione/Trasparenza, controllo di gestione, Provveditorato e Utenze, ha istituito un albo di operatori economici da interpellare per l'affidamento di servizi, lavori e forniture ai sensi degli artt. 36 e 63 del D. Lgs. n. 50/2016;

Visto l'art. 37 comma 1 del d.lgs. 50/2016, il quale stabilisce che le stazioni appaltanti, fermi restando gli obblighi di utilizzo di strumenti di acquisto e di negoziazione, anche telematici, previsti dalle vigenti disposizioni in materia di contenimento della spesa, possono procedere direttamente e

autonomamente all'acquisizione di forniture e servizi di importo inferiore a 40.000 euro e di lavori di importo inferiore a 150.000 euro, nonché attraverso l'effettuazione di ordini a valere su strumenti di acquisto messi a disposizione dalle centrali di committenza;

Ritenuto necessario, procedere all'affidamento in oggetto alla impresa individuale Scalone Giorgio, che ha offerto il servizio richiesto per l'importo di € 6.100,00 (IVA 22% inclusa) dando atto che il mancato impegno può comportare l'inadempienza dell'Ente rispetto ad obblighi di legge, creando danno grave e certo all'Ente;

Visto l'art. 192 del TUEL, in base al quale la determinazione a contrattare deve indicare: il fine che con il contratto si intende perseguire, l'oggetto del contratto, la sua forma, nonché le modalità di scelta del contraente;

Dato atto che ai fini degli adempimenti di cui all'art. 3 della Legge 13 agosto 2010 n. 136, il presente provvedimento è identificato con il **CIG:** Z3C23BFB9C;

Rilevato che in conformità a quanto previsto dall'art. 26 comma 3 bis del D.Lgs. n. 81/2008 non è necessario redigere il DUVRI in quanto trattasi di servizi di natura intellettuale;

Acquisiti:

- la dichiarazione sostitutiva dell'impresa relativa al fatto che la stessa svolge attività d'impresa commerciale in forma individuale senza collaboratori o dipendenti e pertanto non è soggetta all'iscrizione inail;
- documento di verifica dell'assenza dello stato di fallimento, acquisito telematicamente dal Registro delle Imprese archivio ufficiale della CCIAA di Ragusa attestante che la ditta non ha alcuna procedura concorsuale in corso o pregressa;
- richiesta informativa antimafia prot. PR_RGUTG_Ingresso 0012725_20180525;
- autocertificazione dell'impresa sulla tracciabilità dei flussi finanziari ed in particolare contenente il numero di conto corrente dedicato all'affidamento;

Visto il D.Lgs. 18 agosto 2000, n. 267, del TUEL, ed in particolare:

- l'art. 107 che assegna ai dirigenti la competenza in materia di gestione, ivi compresa l'assunzione di impegni di spesa;
- l'art. 151, comma 4 sull'esecutività delle determinazioni che comportano impegno di spesa;
- l'art. 183 che disciplina le procedure per l'assunzione di impegni di spesa;

Visto il punto 8 dell'allegato n. 2 al DPCM 28/11/2011 "Principio contabile applicato concernente la contabilità finanziaria";

Visto il Nuovo Codice degli Appalti D.Lgs.n. 50/2016 che sostituisce il D. Lgs. n. 163/2006, ed il Regolamento di attuazione D.P.R. n.208/2010, la L.R. n.12 del 12 Luglio 2012, il Decreto del Presidente della Regione Sicilia n.13 del 31/01/12;

Ritenuto di provvedere, contestualmente all'adozione del presente provvedimento, agli obblighi di pubblicazione dei dati nella sezione "Amministrazione Trasparente" del sito web dell'Ente, in conformità a quanto previsto dal Decreto Legislativo n. 33 del 14 marzo 2013 e ss.mm.ii.;

Visto il Codice di Comportamento del Comune di Scicli, approvato con deliberazione di Giunta Comunale n. 10 del 31/01/2014;

Visto il Piano triennale per la prevenzione della Corruzione e Piano Triennale per la trasparenza ed integrità 2017- 2019 del Comune di Scicli, approvato con deliberazione della Giunta Comunale n. 16 del 31/01/2018;

Visto il vigente Regolamento Comunale di Contabilità approvato con delibera della Commissione Straordinaria con i poteri del Consiglio Comunale n. 10 del 30/07/2015;

Vista la determina del Sindaco n. 50 del 29/12/2017 e successiva n. 1 del 05/01/2018 di nomina dei titolari delle posizioni organizzative;

Visto l'art. 48 dello Statuto Comunale;

DETERMINA

Per la causale in premessa:

1) di approvare l'offerta, acquisita al protocollo generale dell'Ente in data 25/05/2018 al n. 16507, della impresa individuale Scalone Giorgio, che si allega al presente provvedimento per costituirne parte integrante e sostanziale (**allegato A**);

2) di affidare, conseguentemente, per le ragioni indicate in premessa, che qui si intendono integralmente richiamate, il servizio per l'adeguamento del sistema di gestione della privacy del Comune di Scicli alle disposizioni del nuovo Regolamento Europeo 2016/679 sul trattamento dei dati e contestuale incarico per RDP, alla impresa individuale Scalone Giorgio (P.I. 01490400882; Via Alcide De Gasperi n. 26 - 97100 - RAGUSA) per un importo complessivo di € 5.000,00 oltre IVA 22%, pari a € 6.100,00 IVA 22% compresa.

3) di impegnare la complessiva somma di € 6.100,00 (IVA 22% compresa), occorrente per le finalità di cui al presente provvedimento, alla Missione 1 – Programma 11 – Titolo 1 – Macro aggregato 03 – Cap. 135, del Bilancio di previsione finanziario 2017/2019, annualità 2018;
3) di stabilire che, ai sensi dell'art.192 del TUEL, gli elementi indicati del contratto e della procedura contrattuale sono:
- fine che si intende perseguire: adeguamento dell'Ente alle disposizioni del nuovo Regolamento Europeo 2016/679;
- oggetto del contratto: affidamento del servizio per l'adeguamento del sistema di gestione della privacy del comune alle disposizioni del nuovo regolamento europeo 2016/679 sul trattamento dei dati e contestuale incarico per RPD;
- forma del contratto: lettera commerciale secondo l'uso del commercio ai sensi dell'art. 32 comma 14 del Codice;
- scelta del contraente: affidamento diretto ai sensi dell'art. 36 comma 2 lettera a) del D.Lgs. n. 50/2016;
4) di dare atto che il **CIG** è: Z3C23BFB9C
5) di fare obbligo all'impresa individuale Scalone Giorgio di assumere tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3 della legge 13/08/2010 n. 136..
6) di dare atto che il contratto conseguente al presente provvedimento non è soggetto al termine dilatorio previsto dall'art. 32 comma 10 del D.Lgs. n. 50/2016;
7) di approvare il seguente cronoprogramma di spesa sulla base delle norme e dei principi contabili di cui al D.Lgs 23/06/2011, n. 118 (armonizzazione sistemi contabili), del DPCM 28/12/2011 e delle disposizioni correttive e integrative del D.lgs 126/2014:

ANNO REGISTRAZIONE 2018 TOTALE REGISTRAZIONE € 6.100,00
NUMERO IMPEGNO _____ DATA IMPEGNO _____

ANNO IMPUTAZIONE	IMPORTO IMPUTAZIONE	CONTROLLO CASSA
2018	€ 6.100,00	
TOTALE	€ 6.100,00	

8) di dare atto che il presente impegno di spesa, ai sensi dell'art. 163, comma 2 del TUEL, scaturisce dalla esigenza di adempiere indefettibilmente agli obblighi di legge onde evitare che siano arrecati danni patrimoniali certi e gravi all'Ente in conseguenza della irrogazione delle sanzioni previste in caso di inottemperanza.
9) **di dare atto** che si provvederà alla liquidazione con successivo atto, su presentazione della fattura relativa alla fornitura, tenendo conto delle disposizioni in materia di scissione dei pagamenti (split payment) previsti dall'art. 1, comma 629, lett. b), della Legge 23 Dicembre 2014, n. 190 (Legge di Stabilità 2015).
10) di dare atto dell'assenza di conflitto di interesse anche potenziale in merito all'adozione del presente provvedimento da parte della scrivente e del Responsabile del procedimento e di situazioni che possano dare luogo ad obbligo di astensione ai sensi del D.P.R. 62/2013 e del Codice di Comportamento interno;
11) di dare atto che il presente provvedimento sarà pubblicato all'Albo Pretorio on line dell'Ente per 15 gg. consecutivi nonché nella sezione "Amministrazione Trasparente", ai sensi del D.Lgs. n. 33/2013 e ss.mm.ii;
12) di individuare ai sensi dell'art. 31 del D. Lgs. n. 50/2016, quale Responsabile del Procedimento il sig. Miceli Giombattista, responsabile del Servizio CED.
13) di trasmettere copia della presente determinazione al Settore Finanze per i conseguenti adempimenti di competenza.

Il Capo Settore Amministrativo
Dott.ssa Valeria Drago

- SERVIZIO FINANZIARIO -

IMPEGNO: N. 400/2018
Visto: Si attesta la regolarità contabile e la relativa copertura finanziaria.

Scicli, lì 25/05/2018

IL CAPO SETTORE III ENTRATE-FINANZE
(Dott.ssa Grazia Maria Galanti)

ALL. A)

SG di GIORGIO SCALONE
VIA A. DINATALE 18
97100 RAGUSA
P.IVA 01490400882

GDPR

Il regolamento generale sulla protezione dei dati (GDPR) è il più recente quadro dell'Europa che entrerà in vigore nel maggio 2018. È destinato a sostituire le leggi locali in materia di protezione dei dati come la Data Protection Act del Regno Unito 1998, la Privacywet belga o il Bundesdatenschutzgesetz tedesco (BDSG) .

L'obiettivo primario del GDPR è quello di rafforzare la protezione della sicurezza e della privacy per gli individui. Mentre la PPRR condivide molti principi dai suoi predecessori, costituiti da 11 capitoli, 99 articoli e 187 considerando, non è affatto un piccolo adattamentc.

Dove si Applica il GDPR

Il GDPR si applica a tutti i controller e processori di dati. Vi sono specifici obblighi giuridici posti sui processori e i controllori a livello di DPP. Esso si applica ai processi realizzati da organizzazioni all'interno dell'UE e da organizzazioni al di fuori dell'UE che forniscono prodotti o servizi a privati all'interno dell'UE.

Essa si concentra principalmente sui singoli dati definiti in due categorie di "dati personali" e "dati personali sensibili".

I dati personali comprendono dati individuali e tutte le informazioni che possono essere utilizzate come identificatori in linea, ad esempio un indirizzo IP. I dati personali sensibili lanciano una rete più ampia e coprono dati come dati biometrici o genetici.

Cosa significa il GDPR per le imprese e per gli enti pubblici

Per rispettare il GDPR, le imprese e gli enti pubblici dovranno attuare una serie di misure e controlli sulla sicurezza e la privacy, quali:

- Assegnazione di un responsabile della protezione dei dati
- Notifica di violazione dei dati entro 72 ore
- Inventario di tutti i dati personali trattati
- Protezione dei dati per progettazione e per impostazione predefinita
- Valutazioni d'impatto sulla privacy dei dati
- Ammende fino a 20 milioni di euro o al 4%.

Cosa significa da una prospettiva pratica?

Se non hai ancora gli strumenti e i controlli necessari per la sicurezza, la tua organizzazione dovrà implementare diversi nuovi controlli, politiche e procedure di sicurezza. Sarà inoltre necessario dimostrare la conformità con il DPPR.

Per le organizzazioni di sicurezza e privacy, la nuova regolamentazione non dovrebbe portare troppo a livello tecnico. Per coloro che non hanno, l'impatto sarà molto più grande.

L'art. 33 del **Regolamento Europeo 679/2016 (GDPR)** impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro settantadue ore dal momento in cui ne viene a conoscenza.

SG di GIORGIO SCALONE
VIA A. DINATALE 18
97100 RAGUSA
P.IVA 01490400882

Già attualmente sussiste l'obbligo di notifica delle violazioni di dati personali per particolari categorie di titolari (società telefoniche ed internet provider; pubbliche amministrazioni) o per particolari categorie di trattamenti (sistemi biometrici, dossier sanitario)

La novità del GDPR, che diverrà applicabile dal 25 maggio 2018, è l'estensione dell'obbligo a tutti i titolari.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, settantadue ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR, il cui importo può arrivare a 20.000.000 di euro o al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Occorre in ogni caso tenere conto che, la mancata notifica e/o comunicazione, possono rappresentare per l'autorità di controllo un indizio di carenze più profonde e strutturali quali ad esempio carenze od inadeguatezza di misure di sicurezza, in tal caso, trattandosi di ipotesi separate ed autonome, l'autorità procederà per l'ulteriore irrogazione di sanzioni.

Il rispetto degli obblighi di notifica (art. 33) e di comunicazione (art.34), in situazioni già mediamente complesse (in termini di dimensioni ed articolazione dell'organizzazione del titolare e/o in termini di numero di interessati di cui sono trattati i dati personali e/o in termini di operazioni di trattamento, o di quantità, varietà, natura dei dati trattati), richiede al Titolare di strutturare il trattamento dei dati personali avvalendosi di un sistema di conformità e gestione del rischio che preveda un sotto-sistema per la gestione degli incidenti e la continuità operativa.

Questo sistema deve essere in grado di rispettare i requisiti di trasparenza, evidenza e responsabilità prescritti dal GDPR; si ricorda che l'art.24 punto 1 del GDPR richiede al titolare di "mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR".

Per **"Violazione di dati"** si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

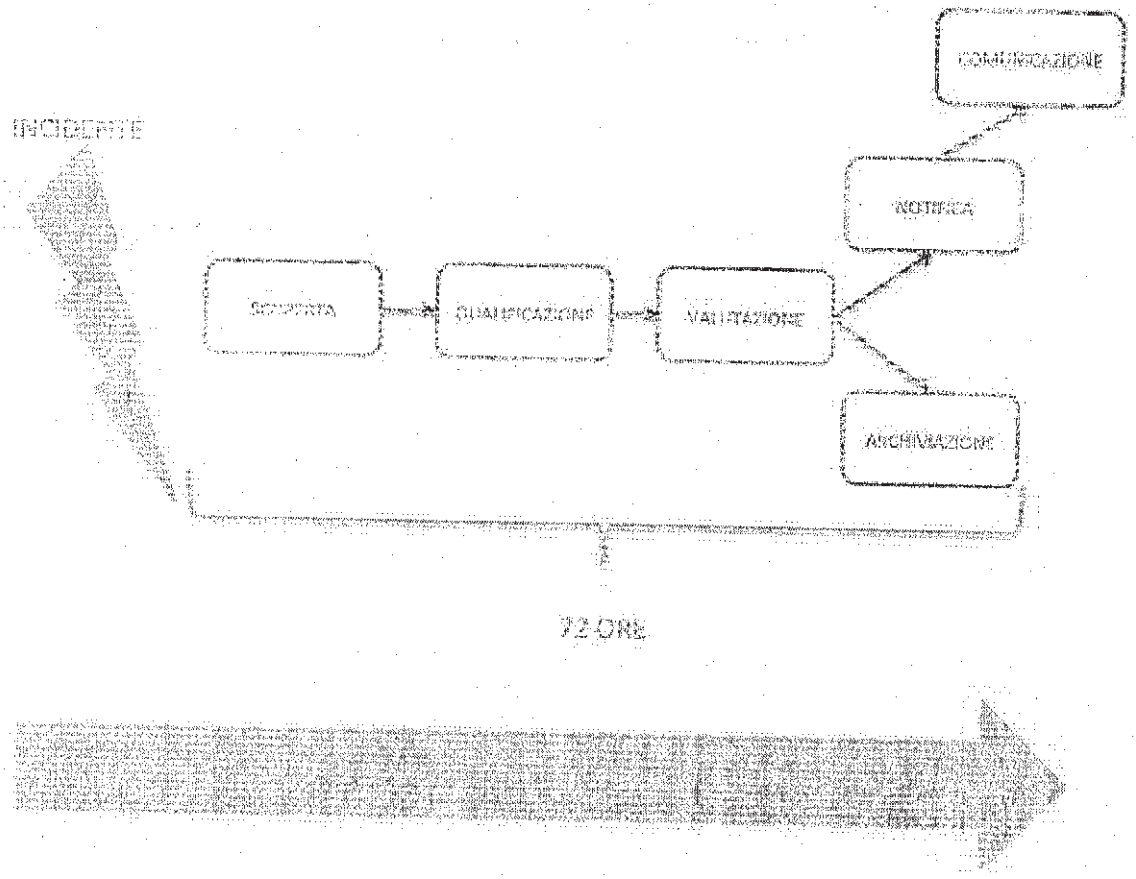
Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR, prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

Ne discende che le generali attività di scoperta dell'incidente, come le successive di trattamento, devono essere documentate, adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

SG di GIORGIO SCALONE
VIA A. DINATALE 18
97100 RAGUSA
P.IVA 01490400882



Il considerando 85 del GDPR spiega che lo scopo della notifica è di limitare i danni che possono derivare per effetto di una violazione a carico degli interessati e che l'efficacia di questo dovere di limitazione dipende dalla tempestività e dall'adeguatezza con cui la violazione è affrontata.

Il gruppo "Article 29 Data Protection Working Party" (WP29)[1], chiarisce ulteriormente che la responsabilità del titolare deve essere commisurata secondo la sua capacità di scoprire tempestivamente un incidente ed indagarlo al fine di valutare l'obbligatorietà della notifica.

Dato che l'obbligo di notifica spetta al titolare, è molto importante che, nell'affidare servizi a responsabili del trattamento, questi, preliminarmente, si accerti della capacità del fornitore nel gestire tempestivamente e adeguatamente un incidente di sicurezza (art. 28 p.1 GDPR) e, quindi, preveda idonee clausole contrattuali (art. 28 p.3 GDPR) che regolino il rapporto di fornitura in modo da garantire il rispetto del GDPR.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

Scoprire l'incidente non è sufficiente, il titolare deve essere in grado di valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati.

Si possono distinguere tre tipi di violazioni:

1) violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.

2) Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.

3) Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

In particolari circostanze le violazioni potrebbero essere combinate tra loro.

Particolarmente "insidiosa" è il terzo tipo di violazione in considerazione dell'eventualità in cui l'indisponibilità sia solo temporanea: deve essere considerata una violazione? In caso positivo quando scatterebbe l'obbligo di notifica?

L'art. 32 del GDPR richiede al titolare di mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; in particolare:

– la lettera b) richiede: "la capacità di assicurare su base permanente la disponibilità dei sistemi e dei servizi di trattamento;

– la lettera c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Da quanto sopra si ricava che un incidente che determini la non disponibilità di dati per un periodo di tempo deve essere comunque considerato violazione e, dunque, deve essere comunque documentato.

L'obbligo di notifica e quello aggiuntivo di comunicazione devono essere valutati caso per caso in relazione ai diritti ed alla libertà degli interessati.

Per esempio: la temporanea indisponibilità di dati personali per un ospedale potrebbe comportare rischi per i diritti e la libertà delle persone fisiche quando determina la cancellazione di un intervento; mentre, nel caso di una società di comunicazioni un'indisponibilità temporanea di dati che determinasse un ritardo nell'invio di una newsletter non sarebbe causa dell'obbligo di notifica.

Il considerando 85 offre utili elementi per determinare i rischi che possono determinare l'obbligo di notifica, in particolare, occorre valutare la possibilità che la violazione possa causare danni fisici, materiali o immateriali alla persona fisica. La disposizione a titolo d'esempio elenca: perdita del controllo dei dati personali che li riguardano; limitazione dei loro diritti; discriminazione; furto o usurpazione di identità; perdite finanziarie; decifratura non autorizzata della pseudonimizzazione; pregiudizio alla reputazione; perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno economico o sociale significativo per la persona interessata.

L'art. 34 del GDPR stabilisce che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve comunicare la violazione all'interessato senza ingiustificato ritardo.

Il considerando 86 del GDPR chiarisce che l'obbligo di comunicazione risponde allo scopo di consentire all'interessato, qualora sussista una violazione che presenta rischi elevati, di prendere le precauzioni necessarie.

La comunicazione ha un contenuto pressoché identico a quello della notifica

Notifica	Comunicazione
Art. 33 p.3 GDPR	Art. 34 p.2 GDPR
a) Descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le	a) Descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali.

categorie e il numero approssimativo di registrazioni dei dati personali in questione.

b) Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.

c) Descrivere le probabili conseguenze della violazione dei dati personali.

d) Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

b) Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.

c) Descrivere le probabili conseguenze della violazione dei dati personali.

d) Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

La comunicazione dovrebbe essere data direttamente e personalmente agli interessati coinvolti dalla violazione, a meno che ciò comporti sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con la medesima efficacia.

La comunicazione deve essere distinguibile rispetto altre diverse comunicazioni che vengono fatte dal titolare agli interessati, in altri termini, la comunicazione deve essere chiara, inequivocabile e richiamare l'attenzione dell'interessato.

Il rispetto di questi requisiti richiede che il titolare, già prima che si verifichi una causa di comunicazione, considerati i dati che tratta e le categorie di interessati, predisponga un piano specifico di comunicazione.

La comunicazione, pur sussistendo la condizione di rischio elevato, si ritiene soddisfatta quando:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

Mentre per far scattare l'obbligo di notifica è sufficiente che sussista una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, per la comunicazione occorre che tale rischio sia elevato.

Il titolare è dunque tenuto non solo ad individuare e qualificare i rischi connessi a violazioni di dati personali, ma, qualora tali rischi riguardino i diritti e le libertà delle persone fisiche, deve anche procedere ad una valutazione del livello di rischio.

Il considerando 76 del GDPR chiarisce che la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Il WP29 suggerisce ulteriori criteri per permettere una valutazione più accurata

1) Tipo di violazione

2) Natura, sensibilità e volume dei dati personali

3) Facilità di riconoscimento degli interessati

SG di GIORGIO SCALONE
VIA A. DINATALE 18
97100 RAGUSA
P.IVA 01430400882

4) Serietà delle conseguenze per le persone fisiche

5) Caratteristiche specifiche delle persone fisiche

6) Quantità di persone fisiche coinvolte

7) Caratteristiche specifiche del titolare

La valutazione dei rischi non sempre è semplice, il WP29 raccomanda al titolare, in caso di dubbio, di scegliere la strada di maggior tutela procedendo alla notifica. Alla luce di quanto detto ci si domanda come e cosa possa fare il titolare per rispettare gli articoli 33 e 34 del GDPR in vista dell'imminente applicabilità fissata al 25 maggio 2018.

I presidi della notifica e della comunicazione seppure richiedono adempimenti specifici, non possono essere letti ed interpretati correttamente senza considerare la loro correlazione con l'intero GDPR, quali organi di un medesimo corpo.

In particolare sono fondamentali gli articoli 24 e 32 del GDPR, essi impongono ad ogni titolare di:

1) mettere in atto misure tecniche e organizzative adeguate per garantire il rispetto del GDPR;

2) essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR;

3) riesaminare ed aggiornare tali misure quando necessario;

4) garantire un livello di sicurezza adeguato al rischio.

Gli obblighi di cui sopra devono essere valutati tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche propri di ciascun titolare.

E' chiaro che, pur essendo uguali per tutti i titolari europei, questi obblighi assumono aspetti diversi a seconda del titolare. Per esempio: se per il titolare di una piccola organizzazione che tratta piccole e limitate quantità di dati personali non è richiesta una particolare attività di formalizzazione, per il titolare di una organizzazione vasta e complessa che tratta dati personali su larga scala, aventi natura sensibile, è invece richiesta la strutturazione di un vero e proprio sistema di gestione dei dati personali (PDMS) che operi interattivamente e sinergicamente con gli altri sistemi di gestione attivi (Per esempio: i sistemi qualità, ambiente, 231, ecc...).

Il trattamento degli incidenti di sicurezza presuppone, a monte, l'esistenza di un sistema di sicurezza delle informazioni che offre tutti gli strumenti necessari.

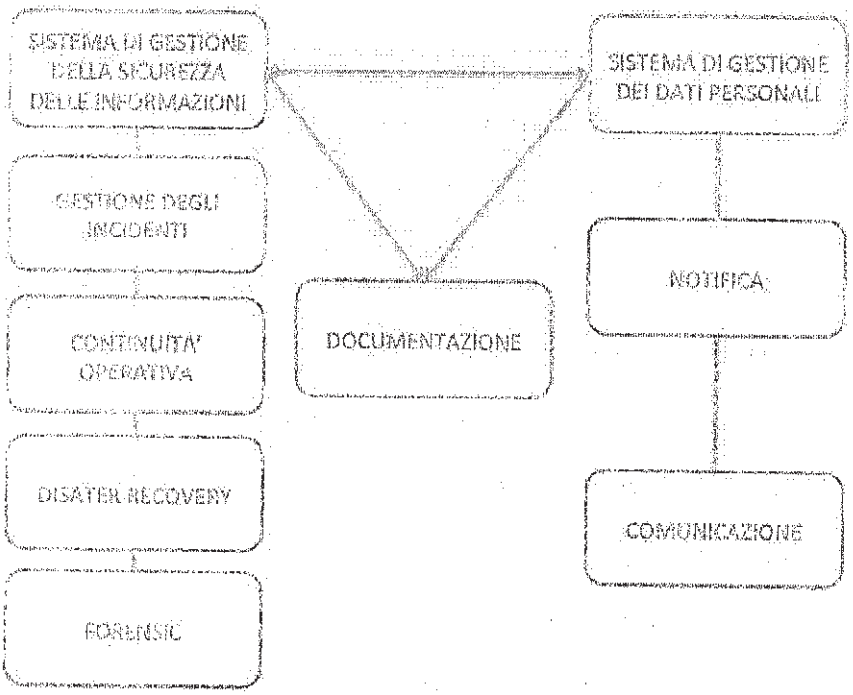
Ad esempio, la scoperta dell'incidente presuppone un sistema di monitoraggio che a sua volta presuppone l'organizzazione della sicurezza all'interno dell'ente (definizione degli obiettivi, politiche, compiti e responsabilità, classificazione di dati e processi, individuazione e definizione dei rischi, individuazione dei rimedi).

La valutazione dell'incidente presuppone la definizione dei criteri di valutazione, la formazione del personale incaricato, la predisposizione di procedure.

La tempestività nella notifica può essere assicurata se preesiste un sistema di comunicazione interno adeguato e tutti coloro che operano per il titolare abbiano ricevuto adeguata formazione.

La stessa comunicazione può essere fatta solo se sono disponibili le informazioni necessarie, aspetto possibile solo se precedentemente è stato strutturato un sistema di report dell'incidente, è stata fatta una ricognizione adeguata dell'organizzazione del titolare, sono state condotte le Valutazioni di impatto sui dati personali (DPIA).

Infine, la stessa documentazione delle violazioni che la norma prescrive di conservare (anche per quelle che non determinano obbligo di notifica), è possibile se è stato strutturato un sistema di gestione degli incidenti.



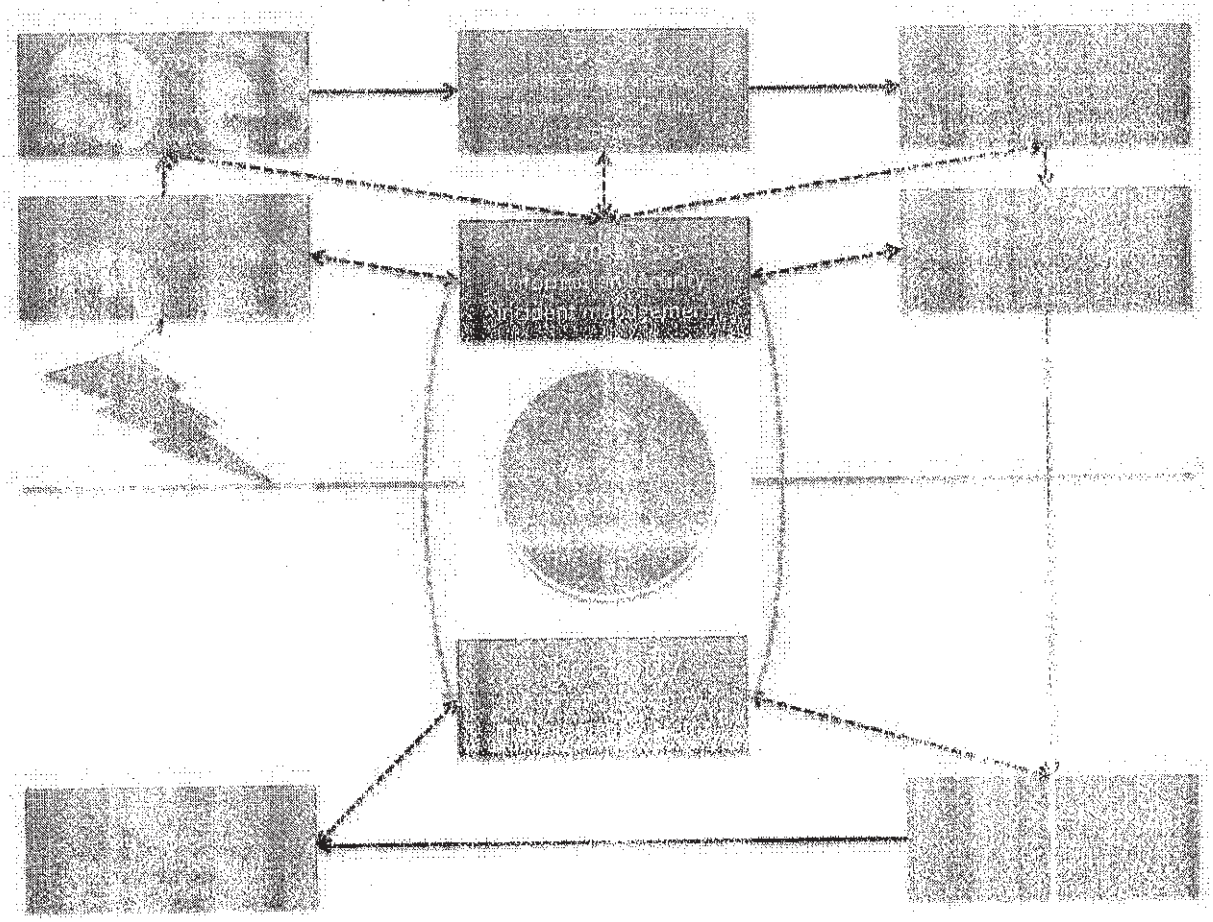
L'aderenza del PDMS a standard e buone prassi, riconosciute (per esempio: UNI – EN – ISO) è certamente un elemento prezioso che aiuta il titolare e ne attesta sia la diligenza che la sensibilità, per titolari che gestiscono organizzazioni complesse, questo passo è fortemente suggerito.

Gli standard internazionali che aiutano a gestire la notifica e la comunicazione sono molteplici, tra questi si segnala:

- ISO 27001: Information security management systems – Requirements.
- ISO 27035 parti 1 e 2: Information security incident management.
- ISO 27043: Incident investigation principles and processes.
- ISO 22301: Business continuity management systems – Requirements.

Lo schema che segue illustra una possibile combinazione degli standard ISO nella gestione della notifica delle violazioni dei dati personali prevista dall'art. 33 del GDPR.

SG di GIORGIO SCALONE
VIA A. DINATALE 18
97100 RAGUSA
P.IVA 01490400882



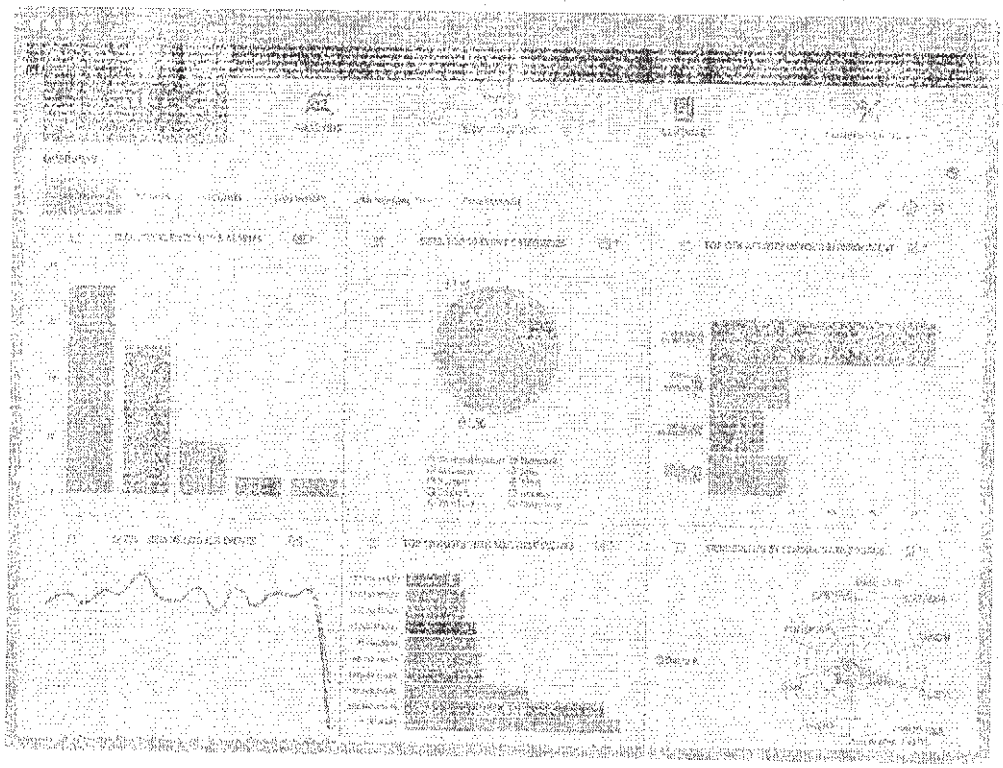
Concludendo, il titolare deve costruire il proprio PDMS estrapolando dagli standard i principi più adatti alle proprie specifiche circostanze, ricordando che il DPMS, pur essendo documentato, non si risolve in tale aspetto, ma rappresenta uno strumento di guida e controllo da utilizzare nella gestione della propria organizzazione.

SG di GIORGIO SCALONE
VIA A. DINATALE 18
97100 RAGUSA
P.IVA 01490400882

Come SG può aiutarti

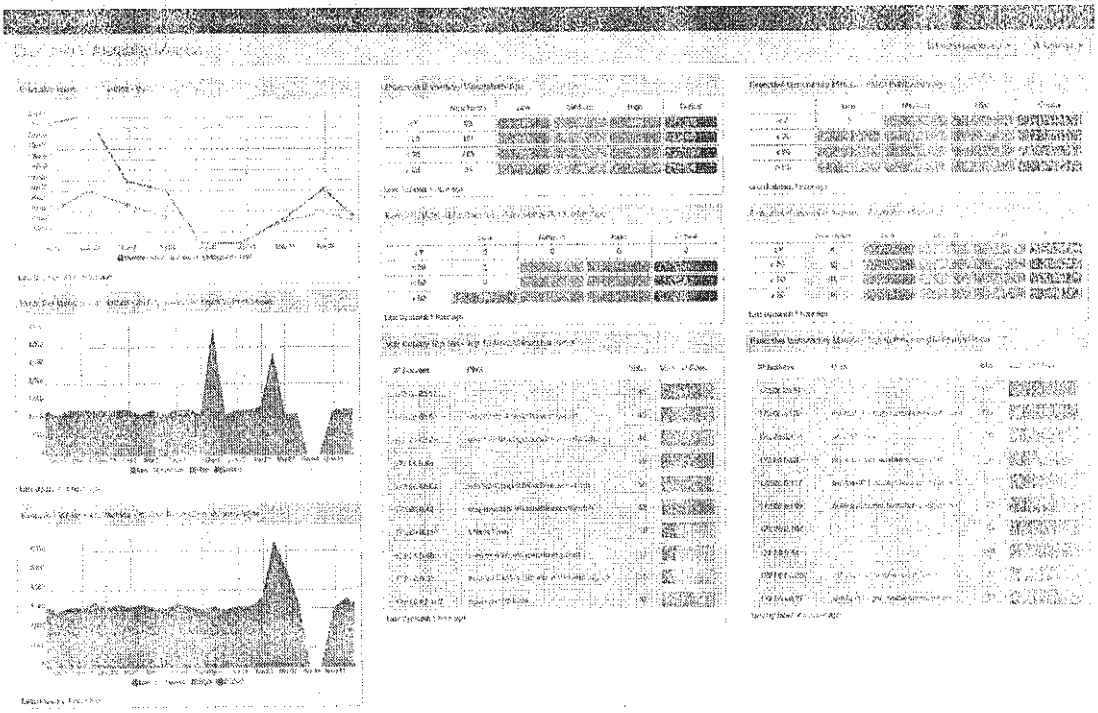
La piattaforma [illegible] ti aiuta a soddisfare molte delle esigenze di sicurezza e privacy della GDPR. Alcune delle funzionalità essenziali integrate nel prodotto includono:

- Scoperta di risorse per rilevare i sistemi sconosciuti sulla rete.

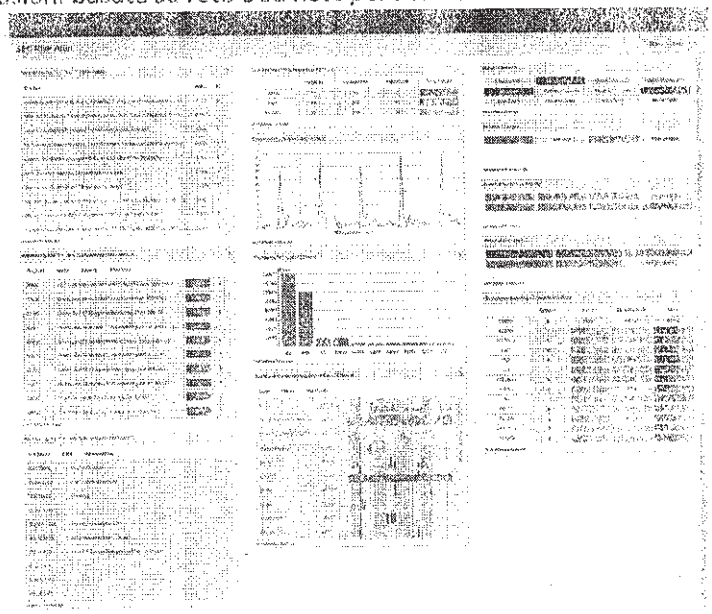


- Valutazione di vulnerabilità per identificare obiettivi probabili da parte degli attaccanti.

SG di GIORGIO SCALONE
VIA A. DINATALE 18
97100 RAGUSA
P.IVA 01490400882

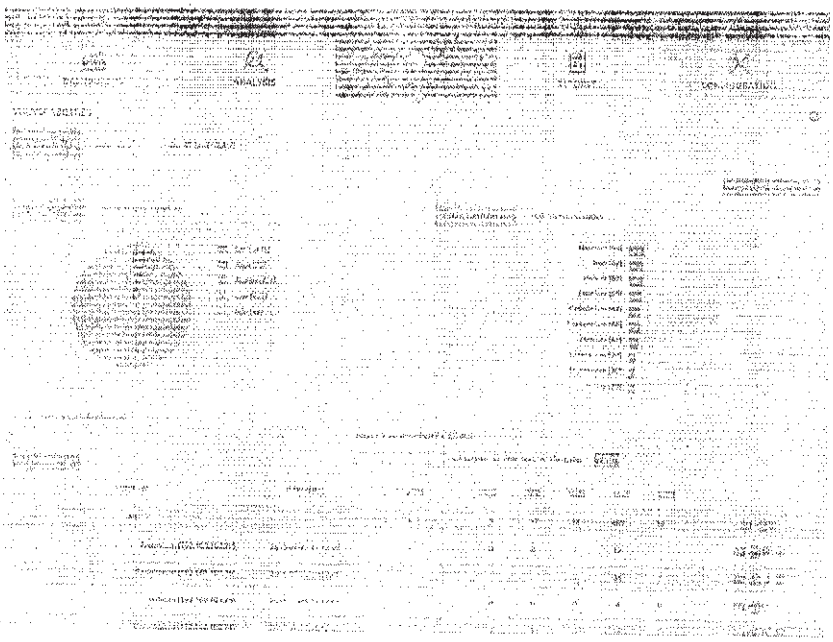


- Rilevamento di intrusioni basate su rete e su host per rilevare attività dannose nella rete.

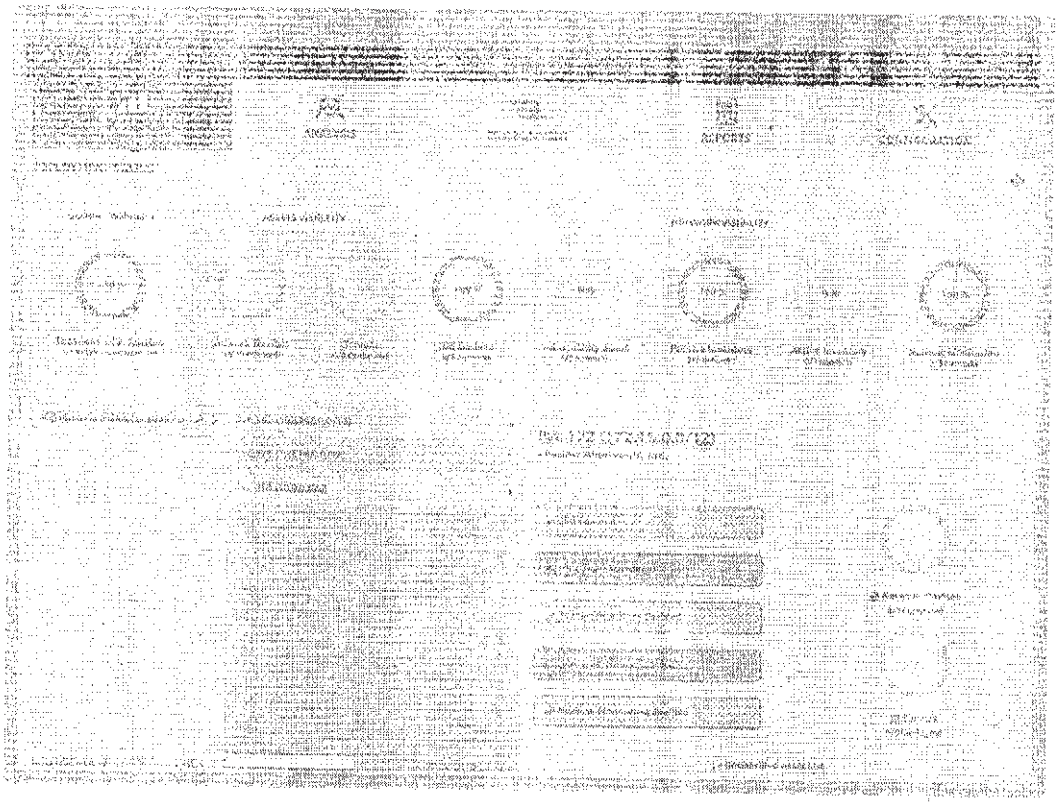


- Monitoraggio dell'integrità dei file (FIM) per rilevare le modifiche nei file critici e l'attività utente sospetta.

SG di GIORGIO SCALONE
VIA A. DINATALE 18
97100 RAGUSA
P.IVA 01490400882

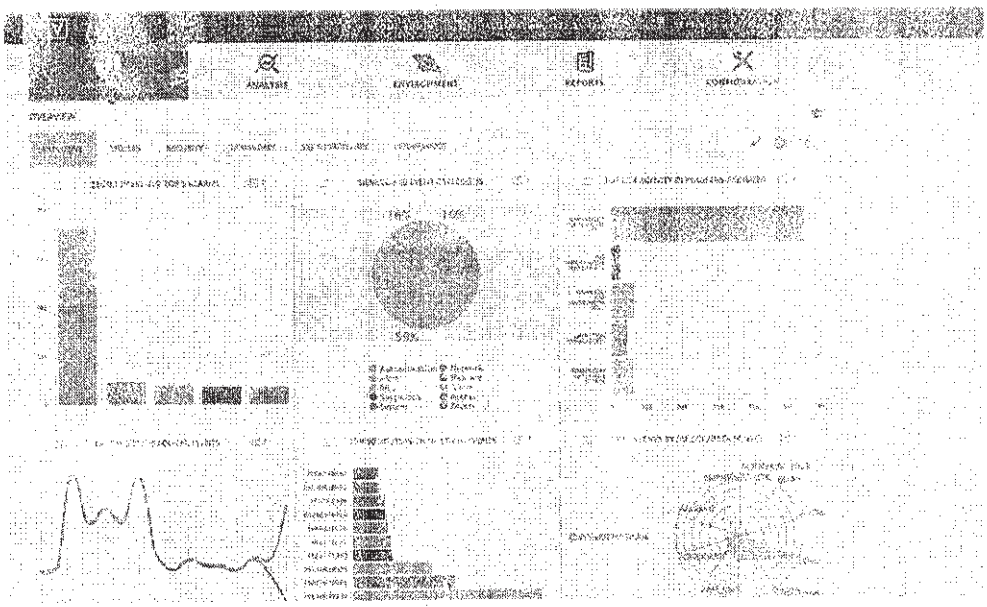


- Gestione log per consentire analisi forense di eventi che utilizzano registri grezzi firmati per la conservazione delle prove.

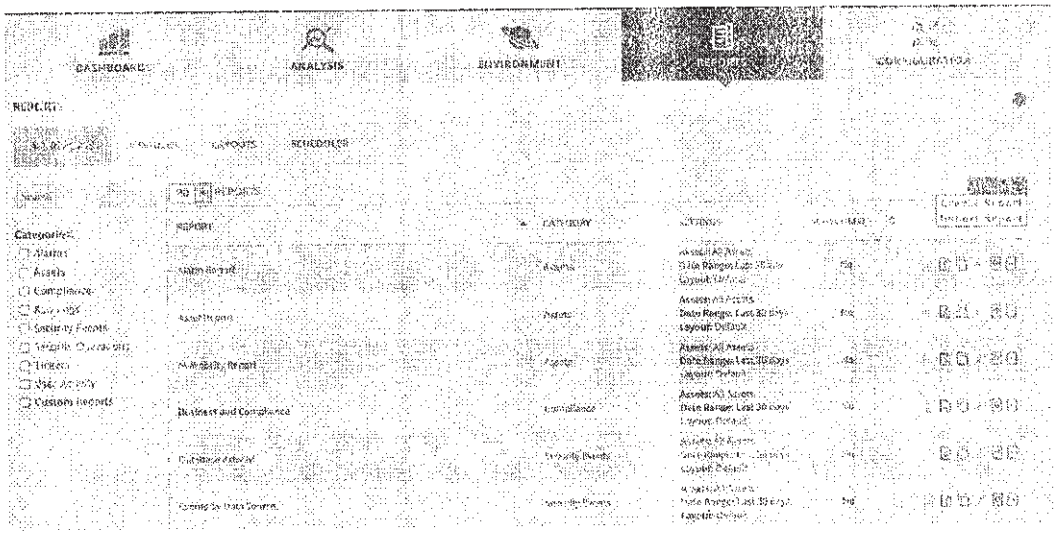


SG di GIORGIO SCALONE
VIA A. DINATALE 18
97100 RAGUSA
P.IVA 01490400882

- Informazioni sulla sicurezza e gestione eventi (SIEM) per correlare eventi di sicurezza da tutta la rete.



- Modelli di rapporto di conformità per GLBA, FFIEC, PCI, nonché report personalizzati.



SG , supportata da Data Protection Officer certificato, ha ideato una soluzione per guidare le aziende nell'intricata galassia dell'applicazione del GDPR:

- Consulenza: introduzione al nuovo GDPR; quali impatti, quali responsabilità, quali sanzioni, approccio metodologico.
- Assessment: analisi dei rischi e dell'impatto del nuovo GDPR sull'azienda, GAP Analysis AS IS - TO BE
- Disegno di processo: consulenza nel disegno di nuovi processi operativi

- Tool di supporto basato sulla struttura organizzativa dell'azienda, identifica i responsabili del trattamento, monitora la correttezza dell'applicazione del GDPR sui processi aziendali, segnala le NON Conformità nel trattamento, suggerisce le azioni correttive necessarie, identifica i Task owner e la data risoluzione delle NC rilevate
- DPO on demand: un servizio di un nostro consulente certificato DPO
    - Mappatura degli archivi elettronici, web e cartacei, individuazione e definizione degli schemi di trattamento dei dati rispetto alle singole unità di archiviazione;
    - Verifica della liceità dei trattamenti, delle modalità tecniche e delle misure di protezione adottate;
- Individuazione dei soggetti interessati al trattamento (utenti, cittadini - persone fisiche e referenti delle persone giuridiche, dipendenti/collaboratori, fornitori, etc.);
- Individuazione delle figure :
    - amministratori di sistema;
    - titolare del trattamento/responsabile del trattamento;
    - affidatari esterni
    - responsabili esterni del trattamento/clausole per l'affidamento di servizi esternalizzati;
    - incaricati al trattamento;
    - fornitori di servizi esterni - verifica ed eventuale integrazioni nella contrattualistica;
- Elaborazione dei documenti
    - Verifica dei requisiti dei fornitori di servizi per i quali vi è un trattamento (e/o implementazione di misure di protezione dei dati) e stesura delle clausole contrattuali minime per garantire adeguata protezione dei dati;
    - stesura delle informative per il trattamento dei dati;
    - stesura del registro dei trattamenti - NUOVO adempimento richiesto dal Regolamento Europeo 2016/679;
    - revisione dell'analisi dei rischi che incombono sui dati - parte vitale del NUOVO adempimento richiesto dal Regolamento Europeo 2016/679;
    - verifica dell'applicazione delle "misure minime" di sicurezza (ex allegato B D.Lgs. n 196/03) e individuazione di ulteriori misure "adeguate".
    - definizione delle modalità di gestione degli adempimenti relativi al Provvedimento a carattere generale del Garante per la protezione dei dati personali inerenti alla figura dell'Amministratore di sistema;
    - eventuali integrazioni di aspetti giuslavoristi inerenti all'utilizzo degli strumenti di lavoro aziendali in affidamento al personale dipendente;
    - verifica ed eventuale integrazione del Regolamento per il trattamento dei dati personali sensibili e giudiziari;

Implementazione di ulteriori documenti:

- checklist per gestire gli adempimenti privacy, manuali per la verifica degli adempimenti eseguiti, piani operativi di verifica dell'attività dei fornitori esterni; mansionari, ecc;
- Audit periodici di verifica dell'adozione delle misure predisposte;
- Formazione degli operatori incaricati e responsabili con rilascio attestato di partecipazione;
- Affiancamento all'ente in sede di verifiche o ispezioni del Garante.

SG di GIORGIO SCALONE
VIA A. DINATALE 18
97100 RAGUSA
P.IVA 01490400882

OFFERTA DPO

COMUNE DI SCICLI
VIA F. MORMINA PENNA 2
97018 SCICLI

Vostro Rif. n.

Codice Fiscale

Partita IVA

A seguito dei contatti intercorsi presentiamo la nostra migliore offerta

Articolo	Descrizione	Qtà	Prezzo	Importo
GDPR001904	STESURA INIZIALE PRIVACY GDPR	1	€ 1.500,00	€ 1.500,00
GDPR0910	Assessment, 150 addetti, 10 applicazioni DB, 30 procedure documenti - Auditor Certificato Schema ISDP 10003:2015 DPO	1	€ 4.500,00	€ 4.500,00

Canone	B.B. SEMESTRALE		€ 6.000,00
Consegna			€ 5.000,00

Ragusa , li 25/05/18

Giorgio Scalone

Luogo di Esecuzione se diverso dall'indirizzo:
I prezzi contenuti nella presente offerta sono al netto di IVA
Validità della presente offerta : 30 gg.

DATA_____ IL CLIENTE _____

(timbro e firma per accettazione)