GDPR
SWASCAN

IL GDPR PER LE PICCOLE E MEDIE IMPRESE

Swascan

The First Cloud Cyber Security
& GDPR Platform

Sommario

1. **GDPR: regolamento generale sulla protezione dei dati**
2. **Trattamento e dato personale**
3. **I dati sensibili**
   - 3.1. I dati sensibili: i dati identificativi
   - 3.2. I dati sensibili: i dati anonimi e pseudo anonimi
4. **Profilazione**
   - 4.1. Il processo decisionale automatizzato
   - 4.2. La differenza tra GDPR e vecchia normativa
5. **Trattamento dei dati: rischi per gli interessati**
   - 5.1. I trattamenti rischiosi
6. **DPIA**
   - 6.1. DPIA: i contenuti
   - 6.2. DPIA: quando è obbligatoria
   - 6.3. DPIA: informazioni aggiuntive
7. **Registro delle attività di trattamento dati: di cosa si tratta?**
   - 7.1. Registro delle attività di trattamento dati: in quali casi è necessario?
   - 7.2. Registro delle attività di trattamento dati: ulteriori specifiche

8. **GDPR: chi sono i player coinvolti**
   8.1. DPO o Data Protection Officer: la figura professionale
   8.2. C'è la necessità di un DPO?
   8.3. Quali sono le conoscenze del DPO?
   8.4. Le responsabilità di un DPO
9. **GDPR: diritti e doveri**
10. **Trattamento lecito e informativa**
   10.1. Informativa: i contenuti
   10.2. Informazioni aggiuntive
   10.3. Informativa: i termini della comunicazione
11. **GDPR: chi è coinvolto? Quali sono le sanzioni?**
12. **GDPR: i passi da seguire per la compliance**
13. **Swascan**
14. **GDPR chiavi in mano**

1

GDPR: REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Il GDPR (General Data Protection Regulation - 2016/679) è il **Regolamento Generale sulla Protezione dei Dati**, il cui testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016, avrà efficacia in tutta l'Unione europea a partire dal **25 maggio 2018**. Con la definitiva entrata in vigore, il Regolamento sostituirà così la Direttiva 95/46/CE abrogando, di conseguenza, le norme del codice sulla privacy (D.lgs. 196/2003) che con esso risulteranno incompatibili. Il Legislatore europeo vuole così definire un **quadro comune in materia di tutela dei dati** personali con l'obiettivo di uniformare la disciplina della Data Protection all'interno dell'Unione Europea e prevenire disparità che possano ostacolare la libera circolazione dei dati nel mercato interno.

La nuova normativa ha inoltre voluto affiancare al principio di territorialità, il **principio di effettività**: i Titolari (anche con sede legale fuori dall'Unione Europea) che trattano i dati di interessati residenti nell'Unione, sono tenuti a porre in essere tutti gli adempimenti imposti dal GDPR. Quest'ultimo impone l'obbligo di nominare preventivamente un proprio rappresentante stabilito nello Stato membro di riferimento, il quale potrà agire in tutte le questioni relative alla Data Protection che riguardano l'entità rappresentata.

Per iniziare, proponiamo una serie di brevi concetti che offrono una panoramica dettagliata della normativa. Si tratta, in poche parole, della **nuova legge che regolamenta il Data Processing e il Data Management**. Questa disposizione legislativa definisce le regole, i modelli e le best practice per la protezione dei dati personali. Per maggior precisione occorre aggiungere che il GDPR fornisce anche una definizione di dati personali. Questa definizione comprende tutte le informazioni relative ad un individuo, connesse alla sua vita sia professionale che privata. Lo spettro è molto ampio: si spazia dai nomi alle fotografie, dall'indirizzo e-mail ai dettagli bancari.

2

TRATTAMENTO E DATO PERSONALE

- L'art. 4 c. 1 definisce come **Dato personale** "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

- L'art. 4 c. 2 definisce come **Trattamento** "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".

3

I DATI SENSIBILI

Nel D.lgs. n. 196/2003 quando si parla di **dati sensibili** si fa riferimento a quei particolari dati che possono rivelare:

- **L'origine razziale ed etnica di un individuo;**
- **Le sue convinzioni religiose, politiche e filosofiche;**
- **Lo stato di salute o la vita sessuale.**

Tuttavia il Regolamento Europeo non parla di dati sensibili, bensì di dati particolari. L'**articolo 9** stabilisce che: "È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l›appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all›orientamento sessuale della persona." Il divieto non si applica in presenza di **consenso esplicito** o di necessità per assolvere gli obblighi. Delle categorie di dati citati dall'articolo, possiamo estrapolare due ulteriori sottocategorie (vita sessuale e salute) che sono considerate **supersensibili**.

Stando a quanto riportato dal GDPR, in questa categoria rientrano anche i dati genetici e biometrici che hanno lo scopo di identificare una persona.

Nel paragrafo 2, tuttavia, vengono elencate le circostanze in cui il trattamento dei cosiddetti dati sensibili è permesso.

"Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

***a)** l'interessato ha prestato il proprio **consenso esplicito** al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;*

*b) il trattamento è necessario **per assolvere gli obblighi ed esercitare i diritti** specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;*

***c)** il trattamento è necessario **per tutelare un interesse** vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;*

***d)** il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;*

***e)** il trattamento riguarda **dati personali** resi manifestamente pubblici dall'interessato;*

f)** il trattamento è necessario **per accertare, esercitare o di-

fendere un diritto *in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali*

g) *il trattamento è necessario* ***per motivi di interesse pubblico*** *rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;*

h) *il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;*

i) *il trattamento è necessario* ***per motivi di interesse pubblico nel settore della sanità pubblica****, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;*

j) *il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato."*

3.1. I DATI IDENTIFICATIVI

Tutto ciò che permette l'identificazione di una persona (dati identificativi) viene detto **PII** (PII, Personally Identifiable Information) e l'insieme racchiude: nome e cognome, indirizzo mail, indirizzo di casa, numero di passaporto, numero di targa del veicolo, numero identificativo personale, numero di patente, numero di passaporto, indirizzo IP (quando collegato ad altri dati), numero di carta di credito, data di nascita, volto, impronte digitali o calligrafia, luogo di nascita, identità digitale, account name o nickname, numero di telefono e informazioni genetiche.

3.2. I DATI ANONIMI E PSEUDO ANONIMI

I dati raccolti possono essere **anonimizzati**, e quindi privati di ogni elemento qualificante come identificativo. Non sono, quindi, assoggettati alla normativa dei dati sensibili in quanto spogliati di identificatività.

Un dato **pseudo-anonimo**, invece, ha il suo elemento identificativo sostituito con un altro elemento che può essere una stringa di caratteri o un nickname. L'identificazione così risulta essere molto difficoltosa e diviene necessaria una chiave di decriptazione. Questi, a differenza dei precedenti, vengono considerati come dati personali. La motivazione risiede nel fatto che – attraverso un altro dato – è possibile risalire all'interessato.

4

PROFILAZIONE

Si tratta di qualsiasi forma di **trattamento automatizzato di dati** consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi ad un individuo, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, l'ubicazione o gli spostamenti di una persona fisica. La profilazione è un trattamento delicato, poiché il risultato è un dato valutativo ottenuto da una macchina artificiale che costruisce sillogismi secondo schemi predeterminati.

4.1. IL PROCESSO DECISIONALE AUTOMATIZZATO

Il processo decisionale automatizzato induce a prendere decisioni solo attraverso mezzi tecnologici e può basarsi su dati forniti direttamente dall'interessato, oppure su dati ricavati da programmi traccianti o dati derivanti da profili precedentemente creati.

4.2. LA DIFFERENZA TRA GDPR E VECCHIA NORMATIVA

Profilazione e processo decisionale automatizzato assumono sfaccettature differenti e rappresentano anche concetti differenti.

Il Codice Privacy all'art. 14 recita:

"*1. **Nessun atto** o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano **può essere fondato unicamente su un trattamento automatizzato** di dati personali volto a definire il profilo o la personalità dell'interessato.*

*2. **L'interessato può opporsi** ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi dell'articolo 17."*

In parole semplici, non prevede che vengano presi provvedimenti (né amministrativi né giudiziari) che implichino una valutazione del comportamento umano svolta in base ad un trattamento automatizzato di dati personali per la definizione del profilo o della personalità dell'interessato. Il comma 2 dello stesso articolo stabilisce che l'interessato può opporsi ad eventuali determinazioni tramite profiling a meno che la determinazione stessa:

- sia **frutto di un contratto** (conclusione od esecuzione);
- venga eseguita **dietro proposta dell'interessato** oppure;
- **rispetti le garanzie** adeguate stabilite dal Codice o da un provvedimento del Garante.

Al contrario del Codice Privacy, l'articolo 22, par. 1 dell'EU GDPR stabilisce che:

"*L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*"

5

TRATTAMENTO DEI DATI: RISCHI PER GLI INTERESSATI

Cosa si intende per rischi ai diritti e alle libertà relativi al trattamento dati? Stando a quanto riportato dal Considerando 75 del GDPR:

"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione

di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati."

5.1. I TRATTAMENTI RISCHIOSI

Quanto stabilito sopra, dunque, rappresenta la discriminante che stabilisce se un trattamento di dati è rischioso o meno per gli interessati. Ogni azienda che effettua trattamenti di dati sensibili deve effettuare una **valutazione dei propri trattamenti** in modo da poter identificare il proprio range operativo in merito alle operazioni di processing.

8 diritti dei soggetti interessati

Swascan

1. DIRITTO AD ESSERE INFORMATI:
(artt. 12, 13, 14) I soggetti interessati devono ricevere, in modo trasparente e accessibile, con un linguaggio semplice e chiaro, tutte le informazioni relative al trattamento relative al trattamento e ai loro diritti.

2. DIRITTO DI ACCESSO:
(art. 15) I soggetti interessati hanno diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni supplementari.

3. DIRITTO DI RETTIFICA:
(art. 16) i soggetti interessati devono poter rettificare i dati forniti in caso di dati imprecisi od incompleti.

4. DIRITTO DI LIMITAZIONE DEL TRATTAMENTO:
(art. 18) i soggetti interessati hanno il diritto di ottenere la limitazione del trattamento in caso di: • dati inesatti • illicietà del trattamento (ed opposizione dell'interessato alla cancellazione dei dati), • in caso di mancato bisogno da parte del titolare dei dati, l'interessato necessita dei dati stessi per l'esercizio o la difesa di un diritto in sede giudiziaria • l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

5. DIRITTO ALLA PORTABILITA':
(art. 20) I soggetti interessati hanno il diritto di ricevere i dati personali forniti al titolare del trattamento e di trasmetterli ad un altro titolare senza impedimenti qualora:
• siano dati trattati con il consenso dell'interessato o sulla base di un contratto
• Il trattamento sia effettuato con mezzi automatizzati

6. DIRITTO DI CANCELLAZIONE:
(art. 17) altrimenti noto come "diritto all'oblio". Questo diritto rappresenta il potere, da parte dei soggetti interessati, di poter richiedere la cancellazione o la rimozione dei propri dati quando non sussistono più le ragioni che giustificano il trattamento dei dati stessi.

7. DIRITTO DI OPPOSIZIONE:
(art. 21) I soggetti interessati possono opporsi:
• a trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, o per il perseguimento di un legittimo interesse del titolare o di terzi, salvo che il titolare ne dimostri la prevalenza rispetto ai diritti dei soggetti interessati • sempre e comunque a trattamenti finalizzati al marketing diretto • a trattamenti finalizzati alla ricerca scientifica o storica o fini a statistici, salvo che siano necessari per l'esecuzione di un compito di interesse pubblico

8. DIRITTI IN RELAZIONE AL PROCESSO DECISIONALE AUTOMATIZZATO E ALLA PROFILAZIONE:
(art. 22) I soggetti interessati hanno diritto di essere informati dell'esistenza di un processo decisionale automatizzato, compresa la profilazione, e di opporvisi salvo che:
• sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento; • sia autorizzato dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; • si basi sul consenso esplicito dell'interessato

Swascan

Via Roma, 55 20060, Cassina De Pecchi (MI) Italy **Tel:** (+39) 02 78620700 **Email:** info@swascan.com

6

DPIA

La DPIA è un importante strumento per valutare se il trattamento sia o meno rischioso. Ma cosa si intende per DPIA? DPIA è l'acronimo che sta ad indicare **Data Protection Impact Analysis**. Di cosa si tratta in concreto? Di una procedura atta a descrivere un trattamento dati e stabilirne così necessità ed adeguatezza oltre che i rischi correlati. Tutto ciò è mirato ad affrontare i rischi stessi in maniera corretta. Non è necessario che la DPIA si concentri su un singolo trattamento, infatti, questa procedura può riguardare trattamenti che presentano analogie e punti comuni in materia di natura, rischi, finalità, modalità.

6.1. DPIA: i contenuti

Stando a quanto riportato dall'articolo 35 del General Data Protection Regulation, la DPIA contiene i seguenti elementi:

- una sistematica **descrizione dei trattamenti** e delle corrispondenti **finalità** oltre che, dove possibile, il **legittimo interesse** del titolare;
- considerando le finalità del trattamento, una **valutazione della proporzionalità e delle necessità**;
- una **valutazione dei rischi** per i diritti e le libertà degli interessati;

• considerando diritti e legittimi interessi degli interessati, le **misure** previste **per affrontare i rischi** includendo le necessarie garanzie di data protection e compliance GDPR.

6.2. DPIA QUANDO È OBBLIGATORIA?

Il tema dell'obbligatorietà della DPIA è probabilmente il più spinoso. A questo proposito, si può riassumere che:

La DPIA è obbligatoria:

> *"Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali."*

In particolare nei seguenti casi:

- valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su trattamento automatizzato e profilazione sulla quale si fondano decisioni che possono implicare conseguenze legali o analoghe per le persone fisiche;
- trattamento su larga scala di categorie particolare di dati (dati sensibili);
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La DPIA **non è obbligatoria** quando:

- i trattamenti non presentano un rischio elevato per i soggetti interessati;
- per un trattamento analogo è già stata condotta una DPIA;
- i trattamenti sono già stati sottoposti a controllo da parte dell'Autorità di controllo entro maggio 2018 e le caratteristiche del trattamento in questione non sono cambiate.

6.3.DPIA: INFORMAZIONI AGGIUNTIVE

La DPIA dev'essere condotta **prima che il trattamento sia in essere**. Si tratta di una valutazione preventiva soggetta ad aggiornamenti periodici e regolari.

La responsabilità della DPIA è del titolare del trattamento, mentre la sua esecuzione pratica è possibile che venga svolta da qualcun altro. Il titolare, comunque, è tenuto a monitorare il processo consultandosi regolarmente con il DPO.

7

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DATI: DI COSA SI TRATTA?

Il registro delle attività di trattamento dati è un importante strumento di compliance aziendale fornito dalla nuova legislazione Europea. Nello specifico, questa documentazione viene regolamentata nell'art. 30 del GDPR: "Registri delle attività di trattamento". Il primo paragrafo di tale articolo fornisce una chiara spiegazione dei contenuti di tale registro.

"Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

***a)** il nome e i **dati di contatto del titolare** del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;*

***b)** le **finalità** del trattamento;*

***c)** una **descrizione delle categorie di interessati** e delle categorie di **dati personali**;*

d) *le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;*

e) *ove applicabile,* ***i trasferimenti di dati personali verso un paese terzo*** *o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*

f) *ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;*

ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1."

7.1. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DATI: IN QUALI CASI È NECESSARIO?

Il paragrafo 2 dell'art. 30 specifica inoltre che:

"*Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:*

a) *il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;*

b) *le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;*

c) *ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*

d) *ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1."*

Viene dunque specificato che ogni responsabile, e qualora ce ne sia uno, il suo rappresentante devono tenere il registro delle attività di trattamento svolte per conto di un titolare del trattamento. Questo passaggio è necessario al fine di garantire la conformità della propria organizzazione alle prescrizioni legislative. Nello stesso paragrafo è inoltre specificato il contenuto di tale registro.

Tuttavia, è necessario specificare che **la tenuta del** registro delle attività di trattamento **dati non è generale**. Non tutte le organizzazioni sono tenute a redigere tale documentazione. Il paragrafo 5 dell'art. 30 a proposito specifica che:

"*Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.*"


E' obbligatorio il registro delle attività di trattamento dati ?
AZIENDA CON PIU' DI 250 DIPENDENTI
NO
I trattamenti possono provocare un danno fisico, materiale o immateriale agli interessati? (discriminazioni, furto o usurpazione d'identità..)
NO
TENUTA DEL REGISTRO CONSIGLIATA
SI
SI
TENUTA DEL REGISTRO OBBLIGATORIA
IL TRATTAMENTO E' DI DATI PARTICOLARI? (dati sensibili art.9 par.1 GDPR)
NO
IL TRATTAMENTO È OCCASIONALE ?
NO
TENUTA DEL REGISTRO OBBLIGATORIA
SI
SI
TENUTA DEL REGISTRO OBBLIGATORIA
TENUTA DEL REGISTRO CONSIGLIATA
Swascan
Swascan
Via Roma, 55 20060, Cassina De Pecchi (MI) Italy
Tel: (+39) 02 78620700
Email: info@swascan.com
START YOUR FREE TRIAL
In collaboration with CISCO

8

Swascan

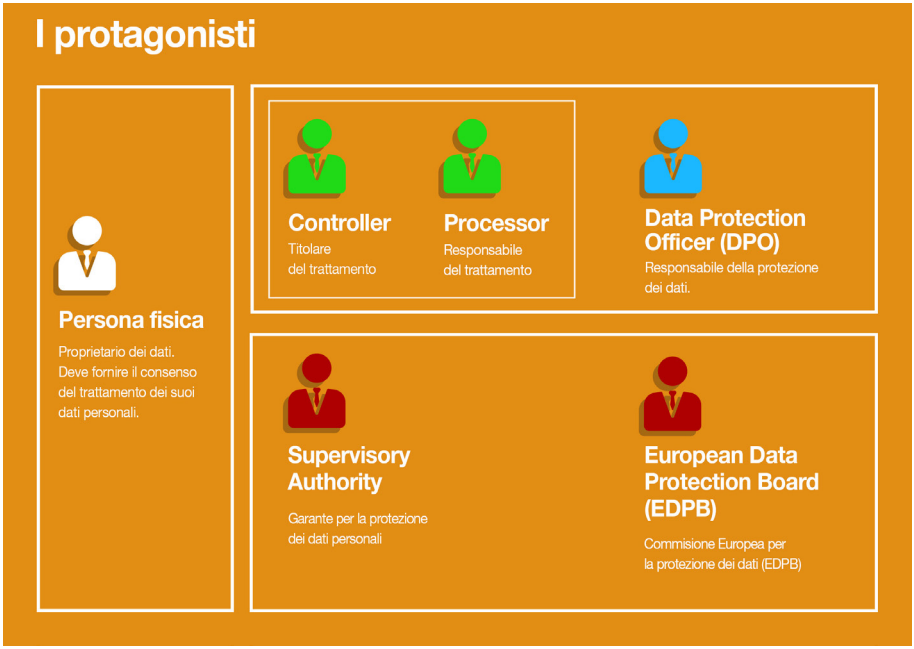
GDPR: CHI SONO I PLAYER COINVOLTI?

Ci sono molteplici figure coinvolte in questi processi. È necessario avere una profonda conoscenza dei ruoli per poter capire al meglio la legge nel suo complesso.

- **Persona fisica**: il proprietario dei dati. Deve fornire un consenso esplicito e scritto per la raccolta e la gestione dei propri dati personali.
- **Controller**: il titolare del trattamento. Il GDPR pone con forza l'accento sulla loro responsabilizzazione (*accountability*), ossia sull'adozione di misure documentabili che assicurino il rispetto delle disposizioni del regolamento. Si assume la responsabilità di comunicare eventuali data breach all'autorità di controllo e agli interessati, mentre il responsabile del trattamento deve informare il titolare del senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
- **Processor**: il responsabile del trattamento. Come per il titolare, il GDPR ne incentiva l'*accountability*. Il responsabile risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. Qualora il titolare e il responsabile siano coin-

volti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni titolare o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

- Data Protection Officer (DPO): si tratta del responsabile della protezione dei dati. È incaricato di avvisare il Controller in caso di vulnerabilità che possano minacciare la protezione dei dati.
- **Supervisory Authority**: il garante per la protezione dei dati personali.
- **European Data Protection Board (EDPB)**.



8.1. DPO O DATA PROTECTION OFFICER: LA FIGURA PROFESSIONALE

L'inserimento del DPO di per sé non rappresenta una novità assoluta. Tuttavia, la sua presenza non era obbligatoria in precedenza. Chi è il Data Protection Officer? Lui / Lei è una figura professionale con abilità specifiche riguardo le leggi e le best practice della protezione dei dati sensibili e non.

8.2. C'È LA NECESSITÀ DI UN DPO?

Ci sono differenti scenari in cui il DPO è obbligatorio ed è nominato sistematicamente dal titolare del trattamento o dal responsabile del trattamento. In quali circostanze specifiche avviene ciò?

1. Quando un'**autorità pubblica** effettua il trattamento (ad eccezione dell'esercizio delle funzioni delle autorità giurisdizionali);
2. Quando il trattamento consiste e richiede il monitoraggio sistematico **su larga scala** degli interessati;
3. Quando il trattamento include, su larga scala, dati sensibili o correlati a procedure penali o reati;

In ogni altra circostanza differente da quelle precedenti è libertà del titolare e del responsabile del trattamento se scegliere o meno un DPO. Inoltre, questi ultimi possono delegare ad un responsabile esterno come un'associazione o una terza parte che possono o meno nominare un DPO.


GDPR
È obbligatorio nominare un Data Protection Officer se :
Swascan
La mia azienda tratta dati personali ?
NO
SI
AZIENDA PRIVATA
AZIENDA PUBBLICA
EFFETTUA MONITORING DEGLI INTERESSATI
PROCESSA DATI SENSIBILI O GIUDIZIARI
Regolarmente e sistematicamente
Viene eseguita una delle seguenti attività:
• Tracciamento e profilazione su internet
• Marketing comportamentale
• Geolocalizzazione
• Email retargeting
• Video sorveglianza
• Telco
• Etc
Swascan
Su larga scala
Per determinarlo dobbiamo considerare:
• Numero di interessati
• Volume dei dati
• Durata del trattamento dei dati
• Perimetro geografico
E' business core ?
NON OBBLIGATORIO
OBBLIGATORIO
Swascan
START YOUR FREE TRIAL
In collaboration with CISCO
Swascan
Via Roma, 55 20060, Cassina De Pecchi (MI) Italy Tel: (+39) 02 78620700 Email: info@swascan.com

8.3. QUALI SONO LE CONOSCENZE DEL DPO?

Un DPO deve poter provare le sue qualità professionali. Innanzitutto, il titolare e il responsabile del trattamento devono considerare la preparazione del DPO in **Data Privacy e Data Processing**. Preparazione sia sul piano teorico che su quello pratico. Un DPO può essere selezionato tra i dipendenti del data controller oppure può essere un freelance. In ogni caso, deve essere noto agli interessati e comunicato alle autorità di controllo competenti.

8.4. LE RESPONSABILITÀ DI UN DPO

Stando a quanto riportato dall'Articolo 39 del GDPR, un DPO ha diversi compiti:

"Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

*1. **informare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;*

*2. **sorvegliare l'osservanza del** presente **regolamento**, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali."*

3. Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'Articolo 35;

4. cooperare con l'autorità di controllo; e

*5. fungere da **punto di contatto** per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.*

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo."

9

Swascan

GDPR: DIRITTI E DOVERI

Il GDPR implica una lunga lista di doveri per le aziende e diritti degli utenti. Per fornire un'overview completa e dettagliata del fenomeno occorre riassumere in punti i temi trattati.

Diritti degli utenti:

- Essere informati riguardo i motivi di **utilizzo dei propri dati personali**: perchè ed in che modo vengono utilizzati i suoi dati?
- Deve avere un accesso libero a tutti i dati che ha fornito. In aggiunta, deve avere la possibilità di trasferire i propri dati da un fornitore ad un altro (**portabilità dei dati**).
- Deve poter richiedere la **modifica**, la **cancellazione** e la **rimozione** dei propri dati. Queste operazioni devono essere facilmente eseguibili (con lo stesso sforzo che si è fatto per concedere i propri dati).
- Essere tempestivamente informato in caso di un **data breach**.
- All'utente deve essere garantito il **rispetto di tutte le leggi in vigore**. Oltretutto, un focus particolare deve essere posto sulle leggi che regolamentano il traffico dei dati fuori dall'Unione Europea.

Doveri delle aziende:

- Provare che l'individuo abbia fornito **esplicito consenso**

per il trattamento dei suoi dati. In aggiunta, devono disporre di questi dati in un modo trasparente ed appropriato.

- Proteggere questi dati dalla **distruzione** accidentale o illegale, dalla loro eventuale perdita e dalla loro eventuale modificazione. Inoltre, le compagnie devono proteggere i dati da accessi e divulgazioni non autorizzate.
- Devono poter provare la compliance alle regolamentazioni attraverso misure di governance. Queste misure includono documentazioni dettagliate e valutazioni del rischio periodiche.
- Notificare entro **72 ore** in caso di data breach.

Punti chiave

Diritti degli Utenti

- Essere informati sui motivi che richiedono la comunicazione dei dati e sulle modalità del loro utilizzo
- Accedere gratuitamente a tutti i dati raccolti e trasferire liberamente i propri dati personali ad altri fornitori di servizi (portabilità dei dati)
- Richiedere la modifica, la cancellazione o la rimozione dei dati, con la stessa facilità con cui hanno espresso il consenso al trattamento
- Essere informati nel caso di una violazione dei propri dati personali
- Avere maggiori garanzie sull'applicazione delle norme e soprattutto sul trasferimento dei dati al di fuori dell'UE

Doveri delle Aziende

- Dimostrare di avere ricevuto un consenso esplicito per tutti i dati personali raccolti
- Utilizzare i dati personali degli Utenti in modo trasparente e appropriato
- Preservare i dati personali dalla distruzione accidentale o illegale, dalla perdita, dalla modifica, dall'accesso e dalla divulgazione non autorizzati
- Adeguarsi alla normativa tramite misure di data governance che includano documentazione dettagliata, registrazione e valutazione continua del rischio
- Notificare entro 72 ore qualsiasi violazione dei dati

10

TRATTAMENTO LECITO E INFORMATIVA

Affinché il trattamento sia lecito è necessario sottoporre all'interessato una specifica informativa. Gli artt. 13 e 14 del Regolamento disciplinano l'informativa nelle seguenti casistiche:

- "*Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*";
- "*Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato*".

10.1. INFORMATIVA: I CONTENUTI

I contenuti dell'informativa collimano quasi perfettamente, sia nel caso in cui dati vengano raccolti presso l'interessato, sia in caso contrario, l'informativa deve contenere:

- *l'**identità** e i **dati di contatto** del titolare del trattamento e, ove applicabile, del suo rappresentante;*
- *i **dati di contatto** del responsabile della protezione dei dati, ove applicabile;*
- *le **finalità del trattamento** cui sono destinati i dati personali nonché la base giuridica del trattamento;*

- *gli eventuali **destinatari** o le eventuali **categorie** di destinatari dei dati personali;*
- *ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.*

Per un singolo punto, però, le informative sono discordanti, infatti, nel caso in cui i dati vengano raccolti **presso l'interessato**, l'informativa deve inoltre contenere:

- *qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i **legittimi interessi** perseguiti dal titolare del trattamento o da terzi.*

In caso contrario (caso in cui i dati **NON** siano **raccolti presso l'interessato**), l'informativa deve contenere:

- *le **categorie di dati personali** in questione.*

10.2. INFORMAZIONI AGGIUNTIVE

Ci sono ulteriori informazioni da specificare nel documento e anche in questo caso queste informazioni dipendono da come sono stati ottenuti i dati:

Dati ottenuti **presso l'interessato**:

1. il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

2. l'esistenza del **diritto** dell'interessato **di chiedere** al titolare del trattamento **l'accesso ai dati** personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

3. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del **diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

4. il diritto di proporre **reclamo** a un'autorità di controllo;

5. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

6. *l'esistenza di un* processo decisionale automatizzato, *compresa la* profilazione *di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.*

Dati **non ottenuti presso l'interessato**:

1. punti **1, 2, 3** e **4** del precedente elenco;

2. *qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i **legittimi interessi** perseguiti dal titolare del trattamento o da terzi;*

3. *la **fonte** da cui hanno origine i dati personali e, se del*

caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

4. *l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.*

10.3. INFORMATIVA: I TERMINI DELLA COMUNICAZIONE

Nel caso in cui i dati **non** siano **ottenuti presso l'interessato**, l'articolo 14 specifica dei termini per la comunicazione, il titolare deve fornire le precedenti informazioni:

- *entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;*
- *nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure*
- *nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.*

11

Swascan

GDPR: CHI È COINVOLTO? QUALI SONO LE SANZIONI?

Chi è coinvolto? Potenzialmente, ogni compagnia, in ogni paese del mondo che raccoglie e tratta dati personali di cittadini europei. Quali sono le **sanzioni**? Dipende, variano da **20 milioni di euro** al **4% del fatturato annuo mondiale totale** dell'anno precedente.

Questo porta a delle semplici ma necessarie domande per essere sicuri di non incorrere in sanzioni.

1. **Quali dati esistono?**
2. **In che modo vengono trattati i dati?**
3. **Dove sono custoditi i dati?**
4. **Chi ha accesso ai dati?**
5. **Quali sono le policy, le procedure e le misure di sicurezza?**

12

Swascan

GDPR: I PASSI DA SEGUIRE PER LA COMPLIANCE

Per rendere più semplice l'argomento, possiamo suddividere i passaggi. Ci sono **6 step** da seguire per ottenere la compliance al GDPR:

1. **Assessment**: effettuare valutazioni a livello di organizzazione, di policy, di processi e di tecnologia.
2. **Analisi del rischio**: analizzare le vulnerabilità ed individuare i rischi a livello di organizzazione, di policy, di processi e di tecnologia.
3. **Valutazione del rischio**: adottare le misure adeguate per la riduzione del rischio, poichè il GDPR non prevede standard minimi.
4. **Attuazione delle misure adeguate**: implementare le misure di sicurezza a livello di organizzazione, di policy, di processi e di tecnologia.
5. **Training**: istruire e sensibilizzare lo staff coinvolto nel processo del trattamento dei dati.
6. **Aggiornamento periodico**: svolgere periodicamente queste attività su base annuale.

GDPR in 6 passi

Cosa dobbiamo fare e... dimostrare di aver fatto

13

SWASCAN: La Piattaforma

La piattaforma Swascan è la suite di Cybersecurity interamente in Cloud, SaaS e Pay for Use che permette di **identificare**, **analizzare** e **risolvere** le criticità, problematiche e vulnerabilità di Sicurezza Informatica degli asset Aziendali a livello di:

- Siti Web
- Applicazioni web
- Mobile App
- Network

Le Funzionalità di Swascan

Web APP SCAN

Security Testing e Security Scan su applicazioni Web per l'identificazione delle vulnerabilità

Analisi vulnerabilità di applicazioni terze che possano generare perdita o accessi indesiderati alla Privacy dei dati

Conformità al modello OWASP e alle normative vigenti

Network SCAN

Network Scan ha l'obiettivo di effettuare lo scan delle vulnerabilità di network e device e suggerire come fixarle

Security Testing e Security Scan a livello di Network

Verifica di conformità con la normativa vigente

Controllo delle procedure interne e policy aziendali

Code Review

La **Code Review** fornisce un'accurata analisi del codice sorgente per identificare le vulnerabilità

Test sulla vulnerabilità del codice sorgente

Individuazione lacunosità ed inefficienza

Identificazione delle aree d'intervento

GDPR Assessment

GDPR Self Assessment Effettua l'analisi e fornisce il livello di Compliance GDPR

GDPR Gap Analysis Identifica le criticità e priorità di intervento

Piano d'azione Determina le attività di riposizionamento

Reporting Generazione automatica di un report pdf.

Swascan è inoltre la soluzione per la gestione della Security Management e per il rispetto dei requisiti previsti dal **Regolamento Europeo Data Protection GDPR** 2016/679 della tua Azienda.

Web app scan

Web App Scan è il servizio automatizzato di Web Vulnerability Scan. Il Tool di Vulnerability Assessment che permette di identificare le vulnerabilità e criticità di sicurezza di siti web e delle applicazioni Web. L'analisi delle vulnerabilità ha lo scopo di quantificare i livelli di rischio e indicare le azioni correttive e di riposizionamento necessarie per il ripristino.

Web Application Scan

Identifica più di 200 tipologie di vulnerabilità delle applicazioni web. Tra queste SQL Injection, Cross-Site Scripting e molte altre.

Owasp

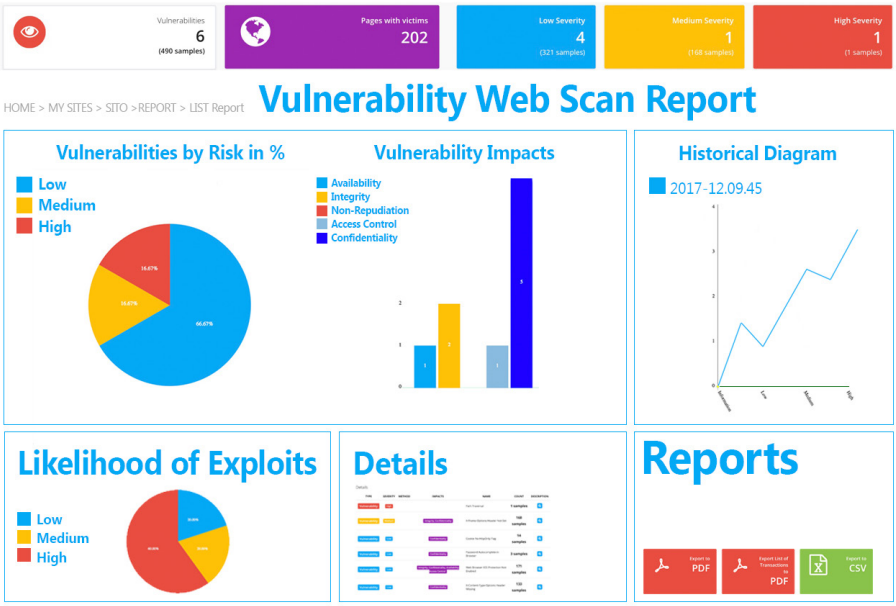
Garanzia di conformità al modello OWASP e alle normative vigenti. Fornisce una analisi dei livelli di rischio unitamente alle indicazioni per la risoluzione delle vulnerabilità.

Security Testing

Security Scan per applicazioni Web per l'identificazione delle vulnerabilità.

Reporting

Generazione automatica di report in pdf e csv.


Vulnerabilities
6
(490 samples)
Pages with victims
202
Low Severity
4
(321 samples)
Medium Severity
1
(168 samples)
High Severity
1
(1 samples)
HOME > MY SITES > SITO >REPORT > LIST Report
Vulnerability Web Scan Report
Vulnerabilities by Risk in %
Low
Medium
High
16.67%
16.67%
66.67%
Vulnerability Impacts
Availability
Integrity
Non-Repudiation
Access Control
Confidentiality
Historical Diagram
2017-12.09.45
Likelihood of Exploits
Low
Medium
High
Details
Reports
Export to PDF
Export List of Transactions to PDF
Export to CSV

Network scan

Network Scan è il servizio automatizzato di Network Vulnerability Scan. Il servizio online di Network Scan permette la scansione dell'infrastruttura e dei device per identificare le vulnerabilità e criticità di sicurezza. L'analisi delle vulnerabilità ha lo scopo di quantificare i livelli di rischio e indicare le azioni correttive e di riposizionamento necessarie per il ripristino.

Network Scan

Effettua il Vulnerability Scan delle vulnerabilità di network e device e suggerisce come fixarle.

Security Testing

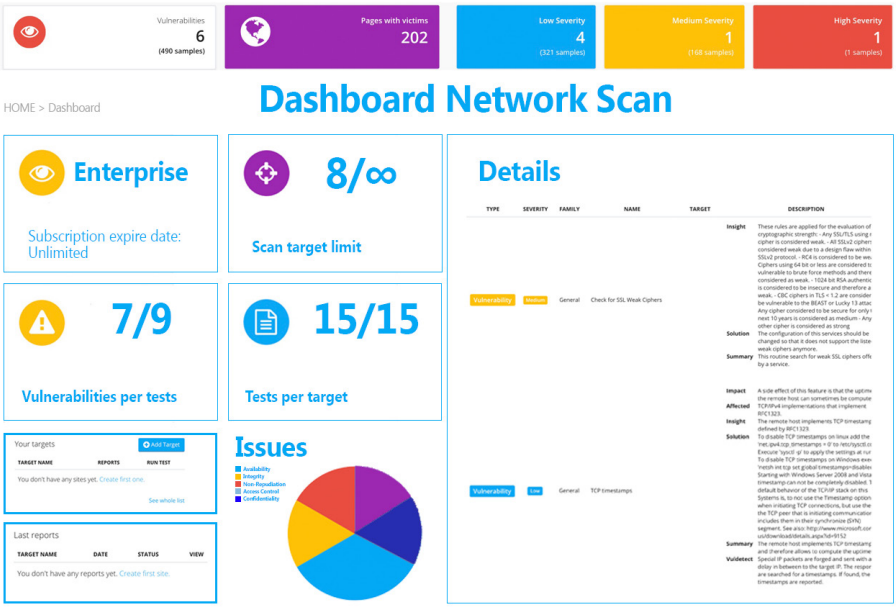
Security Scan delle infrastrutture informatiche.

Compliance

Verifica di conformità con la normativa vigente GDPR. Fornisce una analisi dei livelli di rischio unitamente alle indicazioni per la risoluzione delle vulnerabilità.

Reporting

Generazione automatica di report in pdf e csv.


Vulnerabilities
6
(490 samples)
Pages with victims
202
Low Severity
4
(321 samples)
Medium Severity
1
(168 samples)
High Severity
1
(1 samples)
HOME > Dashboard
Dashboard Network Scan
Enterprise
Subscription expire date:
Unlimited
8/∞
Scan target limit
Details
7/9
Vulnerabilities per tests
15/15
Tests per target
Your targets
Add Target
TARGET NAME
REPORTS
RUN TEST
You don't have any sites yet. Create first one.
See whole list
Last reports
TARGET NAME
DATE
STATUS
VIEW
You don't have any reports yet. Create first site.
Issues
Availability
Integrity
Non-Repudiation
Access Control
Confidentiality

CODE Review

Code Review Scan è il tool automatizzato di analisi statica del codice. Si tratta del processo di analisi del codice sorgente di un'applicazione per verificare che i requisiti minimi di sicurezza necessari siano presenti ed efficaci. La verifica del codice è lo strumento per assicurarsi che l'applicazione sia stata sviluppata in modo da "auto-proteggersi" nel suo ambiente.

Security Code Review

Fornisce un'accurata analisi del codice sorgente per identificare le vulnerabilità e le criticità di security.

Static Code Analysis

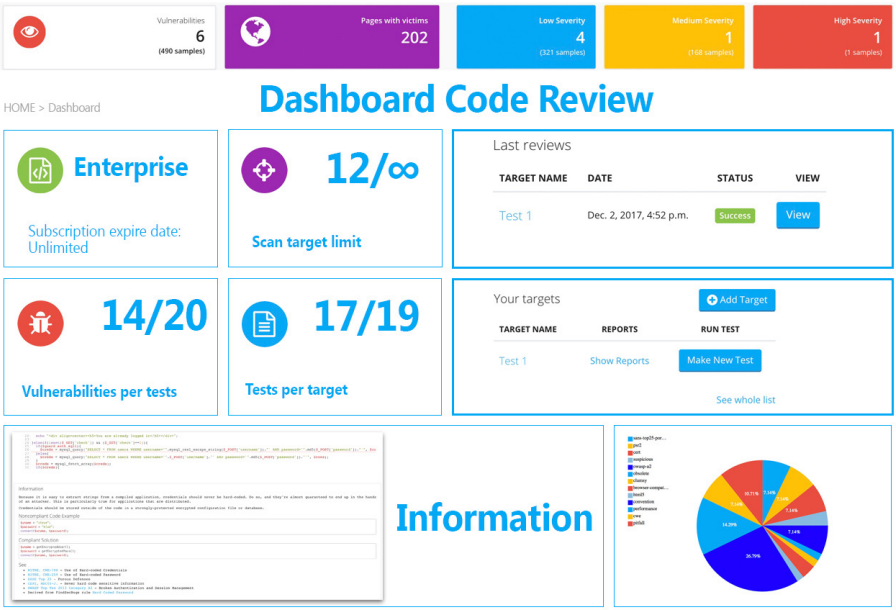
Il Tool di Analisi Statica del Codice Sorgente che supporta oltre 16 linguaggi.

Compliance

Verifica di conformità con la normativa vigente GDPR. Fornisce una analisi dei livelli di rischio unitamente alle indicazioni per la risoluzione delle vulnerabilità.

Reporting

Generazione automatica di report in pdf e csv.


Vulnerabilities
6
(490 samples)
Pages with victims
202
Low Severity
4
(321 samples)
Medium Severity
1
(168 samples)
High Severity
1
(1 samples)
HOME > Dashboard
Dashboard Code Review
Enterprise
Subscription expire date:
Unlimited
12/∞
Scan target limit
Last reviews
TARGET NAME
DATE
STATUS
VIEW
Test 1
Dec. 2, 2017, 4:52 p.m.
Success
View
14/20
Vulnerabilities per tests
17/19
Tests per target
Your targets
Add Target
TARGET NAME
REPORTS
RUN TEST
Test 1
Show Reports
Make New Test
See whole list
Information

GDPR Assessment

GDPR Assessment è lo strumento online che permette alle Aziende di verificare e misurare il proprio livello di compliance rispetto la disposizione legislativa privacy, il General Data Protection Regulation- Regolamento UE 2016/679. Il GDPR Swascan fornisce le indicazioni e azioni correttive da compiere a livello di Organizzazione, Policy, Personale, Tecnologia e Sistemi di Controllo.

GDPR Self Assessment

Effettua un privacy assessment a livello organizzativo, tecnologico e policy/procedure.

GDPR Gap Analysis

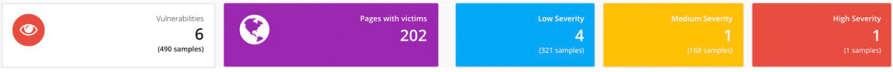
Evidenzia le carenze del sistema di gestione della privacy in uso e definisce le priorità di intervento per l'adeguamento.

Compliance

Determina il livello di compliance fornendo un indicatore di Privacy Compliance.

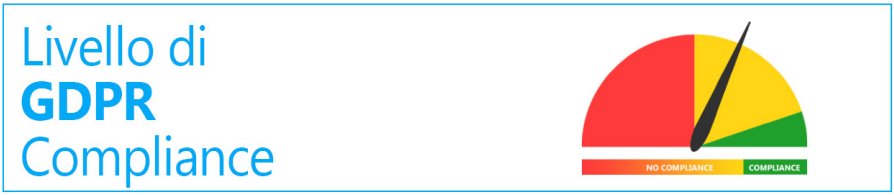
Reporting

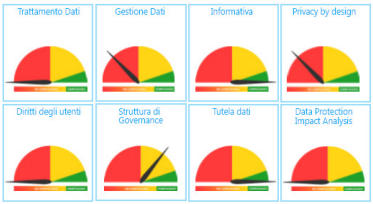
Generazione automatica di un report pdf



HOME > Livello di Compliance GDPR

Livello di GDPR Compliance





Action Plan

Tipo	Severity	Categoria	Descrizione
VULNERABILITY	HIGH	External Redirect	
VULNERABILITY	HIGH	Path Traversal	
VULNERABILITY	HIGH	Remote File Inclusion	
VULNERABILITY	HIGH	SQL Injection	
VULNERABILITY	MEDIUM	Application Error Disclosure	
VULNERABILITY	MEDIUM	Format String Error	
VULNERABILITY	MEDIUM	X-Frame-Option Header Not Set	

14

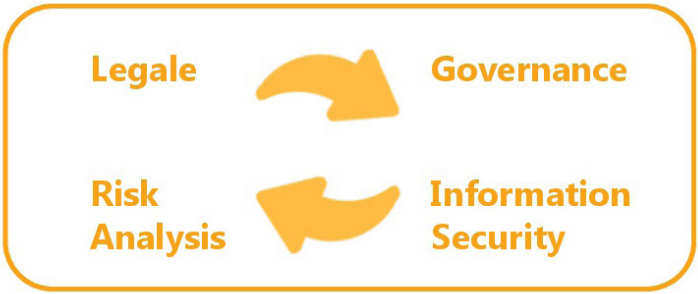
GDPR CHIAVI IN MANO

L'introduzione del nuovo regolamento europeo sulla Data Protection ha provocato significativi cambiamenti per le aziende. Questi cambiamenti in termini di Tecnologia, Organizzazioni, Policy, Personale e Sistemi di Controllo sono mirati al raggiungimento della Compliance. Quali sono dunque gli step da seguire e le attività da intraprendere? È possibile consultare consultare la brochure di Swascan per i servizi GDPR Chiavi in Mano.

Un Team di Competenze per la GDPR
Esperti e Professionisti del Settore

Avvocati e Esperti in ambito **Normativo** e **Legale** nel settore della Privacy e GDPR

Professionisti di **Corporate Governance** con competenze in ambito Business Process Analysis e Policy Framework



Esperti di **Risk Assessment** e **Risk Management** a livello Organizzativo, Processi e a livello tecnologico

CyberSecurity Expert con competenze Nella progettazione e realizzazione di **Sercurity e Data Governance Framework tecnologici**

Consulenza GDPR: professionalità ed esperienza

La consulenza Swascan legata alle tematiche **GDPR** copre diversi settori ed ambiti, tutti presidiati da professionisti con comprovata esperienza:

- ✔ **Legale**: avvocati ed esperti in ambito legale e normativo per quanto riguarda le tematiche GDPR e **Privacy**;
- ✔ **Governance**: professionisti di **Corporate Governance** con competenze in ambito di Business Process Analysis e Policy Framework;
- ✔ **Information Security**: esperti in materia di **CyberSecurity** con competenze nella progettazione e realizzazione di Security e Data Governance Framework tecnologici;
- ✔ **Risk analysis**: esperti di **Risk Assessment** e **Risk Management** a livello Tecnologico, Organizzativo e di Processi.

STEP PER LA GDPR COMPLIANCE

Per adeguarsi alla nuova regolamentazione europea Swascan offre un percorso modulare che affronta il tema della **Compliance** in maniera chiara e diretta.

Si tratta di un percorso strutturato per **FASI** che permette di indirizzare le **attività propedeutiche** alla revisione dei processi organizzativi ed informatici, nel rispetto di quanto richiesto dalla normativa.

Un Percorso Modulare
GDPR Chiavi in mano

Un percorso modulare che permette alle Aziende di adeguarsi al regolamento generale sulla **protezione dei dati** (GDPR)

Un percorso strutturato per **FASI** che permette di indirizzare le **attività propedeutiche** alla revisione dei processi organizzativi ed informatici, nel rispetto di quanto richiesto dalla normativa.

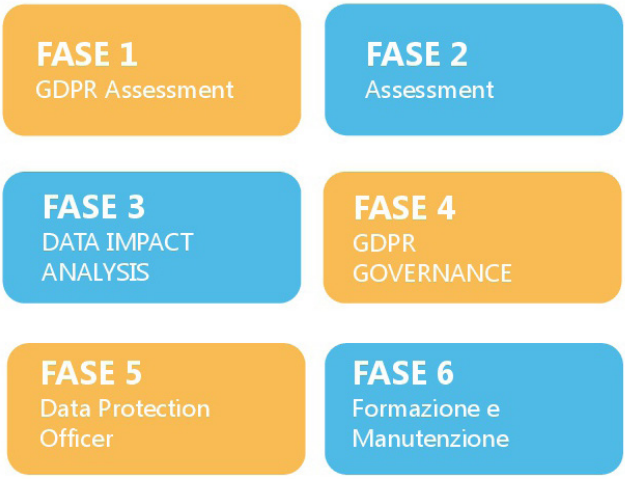
Start to be GDPR Compliant

- Fase 1: GDPR Assessment
- Fase 2: Assessment
- Fase 3: Data Impact Analysis

My Company is GDPR Compliant

- Fase 4: GDPR Governance
- Fase 5: Data Protection Officer
- Fase 6: Formazione e Manutenzione

L' obiettivo è di garantire **l'adeguamento alla normativa** in modo Efficace, Efficiente, Coerente e Sostenibile alla realtà Aziendale



Start to be **GDPR Compliant**:

Fase 1: **GDPR Assessment**

Fase 2: **Assessment**

Fase 3: **Data Impact Analysis**

My company is **GDPR Compliant**

Fase 4: **GDPR Governance**

Fase 5: **Data Protection Officer**

Fase 6: **Formazione** e **Manutenzione**

L'obiettivo è quello di garantire **l'adeguamento alla normativa** in modo Efficace, Efficente, Coerente e Sostenibile alla realtà aziendale.

Un Approccio Modulare al GDPR
Partenza e Arrivo

Start to be GDPR Compliant

Assessment & Risk Analysis

Moduli

- **Start**: GDPR Assessment
- **Assessment:**
  - Data Assessment
  - Assessment Organizzativo
  - Assessment Tecnologico
- **Data Impact Analysis**
  - Risk Analysis Organizzativo/Legale
  - Risk Analysis Tecnologico

Risultati

- Determina il livello di compliance fornendo un indicatore di Privacy Compliance
- Mappatura Trattamenti
- Assessment Organizzativo, Policy e Procedure
- Assessment Tecnologico e ICT Security Measures
- Gap Analysis rispetto alla normativa di riferimento Personal Data Protection trattata dal GDPR sia a livello organizzativo che tecnologico
- Risk Analysis volto a Identificare, Analizzare e Valutare i rischi organizzativi e tecnologici
- Definizione delle attività, e misure organizzative e tecnologiche necessarie per la GDPR Compliance

Un Approccio Modulare al GDPR
Partenza e Arrivo

My Company is GDPR Compliant

Ready to GDPR & Manutenzione

Moduli

- **GDPR Governance**
  - Documentazione Legale
  - Policy & Procedure Framework
  - CyberSecurity Framework
  - Registro Trattamento Dati
  - Data Breach Procedure
- **DPO**
- **Formazione e Manutenzione**

Risultati

- Redazione della Documentazione Legale
- Redazione delle Policy, Procedure e misure di sicurezza aziendali
- Scouting e definizione delle misure di sicurezza ICT
- Redazione del Registro trattamento dei Dati
- Attività di formazione del personale
- Servizio di Data Protection Officer
- Attività di manutenzione e aggiornamento del GDPR Framework

Start to be GDPR Compliant: Assessment & Risk Analysis.

Moduli:

Start: **GDPR Assessment**

Assessment:

- Data Assessment
- Assessment Organizzativo
- Assessment Tecnologico

Data Impact Analysis:

- Risk Analysis Organizzativo / Legale
- Risk Analysis Tecnologico

Risultati:

- Determinare il livello di Compliance fornendo un indicatore di **Privacy Compliance;**
- Eseguire una mappatura dei trattamenti;
- Effettuare un **Assessment** a livello Organizzativo, di Policy e di Procedure;
- Svolgere un Assessment a livello **Tecnologico** e **ICT Security Measures**;
- Fare una **GAP Analysis** rispetto alla normativa di riferimento Personal Data Protection trattata dal GDPR sia a livello Organizzativo che tecnologico;
- Eseguire una Risk Analysis volto ad identificare, analizzare e valutare i rischi **Organizzativi** e **Tecnologici**;

- Definire le attività e le misure Organizzative e Tecnologiche necessarie per la GDPR Compliance.

My company is GDPR Compliant: Ready for GDPR & Manutenzione

Moduli:

GDPR Governance

- Documentazione legale;
- Framework Policy & Procedure;
- CyberSecurity Framework;
- Registro delle attività di trattamento
- Data Breach Procedure

DPO

Formazione e Manutenzione

Risultati:

- Redazione della **Documentazione legale**;
- Redazione delle Policy, Procedure e misure di sicurezza aziendali;
- Scouting e definizione delle **misure di sicurezza ICT**;
- Redazione del **registro delle attività** di trattamento;
- Attività di **formazione** del personale;
- Servizio di **Data Protection Officer**;
- Attività di manutenzione ed aggiornamento del **GDPR Framework**.

Start to Be GDPR Compliant
Assessment & Risk Analysis

GDPR Assessment

Obiettivo

Determinare lo stato dell'arte generale rispetto agli adempimenti Normativi

Risultati

- Determina il livello di compliance fornendo un indicatore di Privacy Compliance
- Evidenzia le carenze del sistema di gestione della privacy in uso e definisce le priorità di intervento per l'adeguamento.

Attività

- Intervista

Output

- Report PDF

Start to Be GDPR Compliant
Assessment & Risk Analysis

Assessment

Obiettivo	Redigere l'inventario dei trattamenti, struttura organizzativa, procedure, policy, misure di sicurezza

Risultati	• Inventario dei trattamenti • Inventario delle finalità e modalità dei trattamenti • Analisi struttura organizzativa • Inventario Policy e Procedure • Inventario Asset fisici coinvolti nel processo di trattamento dati • Inventario Asset Informatici coinvolti nel processo di trattamento dati • Inventario misure di sicurezza • Inventario e Analisi delle Informative/Consensi

Attività	• Intervista • Network Inventory

Output	• Inventario Dati Report PDF • Inventario Governance Report PDF • Inventario Normativo Report PDF • Inventario Tecnico PDF

Start to Be GDPR Compliant
Assessment & Risk Analysis

Data Impact Analysis

Obiettivo	Effettuare la Data Impact Analysis e Determinare la Gap Analysis rispetto alla normativa

Risultati	• Gap Analysis rispetto alla normativa di riferimento Personal Data Protection trattata dal GDPR sia a livello organizzativo che tecnologico • Risk Analysis volto a Identificare, Analizzare e Valutare i rischi organizzativi e tecnologici • Definizione delle attività, e misure organizzative e tecnologiche necessarie per la GDPR Compliance

Attività	• Intervista • Vulnerability Assessment • Network Scan

Output	• Vulnerablity Assessment Report PDF • Network Scan Report PDF • Data Impact Analysis e Risk Analysis Report PDF • Action Plan Report PDF

Di seguito le attività Swascan di Assessment e Risk Analysis:

GDPR Assessment:

Obiettivo:

- Determinare lo stato dell'arte generale rispetto agli adempimenti normativi

Risultati:

- Determinare il livello di Compliance fornendo un **indicatore di Privacy Compliance**;
- Evidenziare le carenze del sistema di gestione della privacy in uso e definire le priorità di intervento per l'adeguamento.

Attività:

- Intervista

Output:

- Reportistica in PDF

Assessment:

Obiettivo:

- Redigere l'inventario dei trattamenti, struttura organizzativa, policy, procedure e misure di sicurezza.

Risultati:

- Inventario dei **trattamenti**;
- Inventario delle **finalità** e delle **modalità** dei trattamenti;
- Analisi della **struttura organizzativa**;

- Inventario di **Policy** e **Procedure**;
- Inventario degli **asset fisici** coinvolti nel processo di trattamento dati;
- Inventario degli **asset informatici** coinvolti nel processo di trattamento dati;
- Inventario delle **misure di sicurezza**;
- Inventario ed analisi delle **informative** e dei **consensi**.

Attività:

- Intervista;
- Network inventory.

Output:

- Inventario **Dati** report in PDF;
- Inventario **Governance** report in PDF;
- Inventario **Normativo** report in PDF;
- Inventario **Tecnico** in PDF.

Data Impact Analysis:

Obiettivo:

- Effettuare la Data Impact Analysis e la GAP Analysis rispetto alla normativa.

Risultati:

- **Gap Analysis** rispetto alla normativa di riferimento Personal Data Protection trattata dal GDPR sia a livello or-

ganizzativo che tecnologico;

- **Risk Analysis** volto ad identificare, analizzare e valutare i rischi organizzativi e tecnologici;
- Definizione delle attività, e misure organizzative e tecnologiche necessarie per la **GDPRCompliance**;

Attività:

- Intervista;
- Vulnerability Assessment;
- Network Scan.

Output:

- **Vulnerablity Assessment** Report in PDF;
- **Network Scan** Report in PDF;
- **Data Impact Analysis** e **Risk Analysis** report in PDF;
- **Action Plan** report in PDF.

My company is GDPR Compliant

My Company is GDPR Compliant
Ready to GDPR & Manutenzione

GDPR Governance

Obiettivo	Predisporre la documentazione legale, policy, procedure e soluzioni tecnologiche per la GDPR Compliance
Risultati	• Redazione della documentazione Legale • Redazione Informative • Redazione Lettere di Incarico • Redazione delle Policy & Procedure • Individua le soluzioni di CyberSecurity • Redazione del Registro Trattamento Dati • Redazione della policy di Data Breach • Redazione policy e procedure di Privacy by Design progettuale
Attività	• Interviste • Redazione documentale • Scouting Tecnologico
Output	• Documentazione Legale – Documenti Word • Documentazione Organizzativa - Documenti Word • Soluzioni Tecnologiche – Documento PDF

My Company is GDPR Compliant
Ready to GDPR & Manutenzione

Data Protection Officer

Obiettivo	Supportare l'azienda fornendo consulenza legale, organizzativa e tecnologica in qualità di Data Protection Officer
Risultati	• Informare il titolare e gli incaricati circa gli obblighi derivanti dai dati trattati • Monitorare l'implementazione ed applicazione delle **politiche** adottate dal titolare in materia di **protezione dei dati.** • Monitorare che **accessi illeciti** ai dati siano notificati dal controller, senza ritardo, nel rispetto della norma, all'autorità Garante • Monitorare l'efficacia, l'adeguatezza e l'applicazione del DPIA • Cooperare con l'autorità **Garante per la Privacy**.
Attività	• Interviste • Audit • Interventi in base alle esigenze
Output	• Report attività effettuate • Report criticità identificate

My Company is GDPR Compliant
Ready to GDPR & Manutenzione

Formazione e Manutenzione

Obiettivo	Formazione del personale e attività di controllo e miglioramento continuo
Risultati	• Attività di formazione del personale aziendale • Attività periodica di Risk Analysis Organizzativa • Attività Periodica di Risk Analysis Tecnologica
Attività	• Formazione in aula • Intervista • Vulnerability Assessment • Network Scan
Output	• Vulnerablity Assessment Report PDF • Network Scan Report PDF • Data Impact Analysis e Risk Analysis Report PDF • Action Plan Report PDF

Di seguito le attività Swascan per la **GDPR Compliance e la Manutenzione:**

Obiettivo:

- Predisporre la documentazione legale, policy, procedure e soluzioni tecnologiche per la **GDPR Compliance**

Risultati:

- Redazione della **documentazione Legale**;
- Redazione delle **Informative**;
- Redazione delle **Lettere di Incarico;**
- Redazione delle **Policy** & **Procedure;**
- Individuare le soluzioni di CyberSecurity;
- Redazione del **registro delle attività** di trattamento dati;
- Redazione della policy in caso di **data breach**;
- Redazione di policy e procedure di **Privacy by Design** progettuale.

Attività:

- Interviste;
- Redazione documentale;
- Scouting Tecnologico.

Output:

- **Documentazione legale** in WORD;
- **Documentazione organizzativa** in WORD;

- **Soluzioni tecnologiche** in PDF.

Data Protection Officer:

Obiettivo:

- Supportare l'azienda fornendo consulenza legale, organizzativa e tecnologica in qualità di Data Protection Officer.

Risultati:

- Informare il titolare e gli incaricati circa gli obblighi derivanti dai dati trattati;
- Monitorare l'implementazione e l'applicazione delle **politiche** adottate dal titolare in materia di protezione dei dati;
- Monitorare che gli accessi illeciti ai dati siano notificati dal controller, senza ritardo, nel rispetto della norma, all'**autorità garante**;
- Monitorare l'efficacia, l'adeguatezza e l'applicazione del **DPIA**;
- Cooperare con l'autorità garante per la privacy.

Attività:

- Interviste;
- Audit;
- Interventi in base alle esigenze.

Output:

- Report delle attività effettuate;

- Report delle criticità individuate.

Formazione e Manutenzione:

Obiettivo:

- **Formazione del personale** e attività di controllo e miglioramento continuo.

Risultati:

- Attività di formazione del personale aziendale;
- Attività periodica di **Risk Analysis Organizzativa**;
- Attività periodica di **Risk Analysis Tecnologica.**

Attività:

- Formazione in aula;
- Intervista;
- Vulnerability Assessment;
- Network Scan.

Output:

- **Vulnerablity Assessment** Report in PDF;
- **Network Scan** Report in PDF;
- **Data Impact Analysis** e **Risk Analysis** report in PDF;
- **Action Plan** report in PDF.

The First Cloud Cyber Security & GDPR Platform

Swascan

WWW.SWASCAN.COM

Swascan Staff

Testi

D'agostino Federico
Parravicini Giovanni
Paglia Riccardo
Dossoni Monica

Grafica

Ebrahem Manuel