“Il GDPR per lo studio professionale”

A cura di Ing. Vito Santarcangelo

Ing. Vito Santarcangelo
PhD St. @ DMI University of Catania
Lead Auditor ISO 27001:2013
CEO iInformatica S.r.l.s.

www.iinformatica.it

iInformatic@ Srls

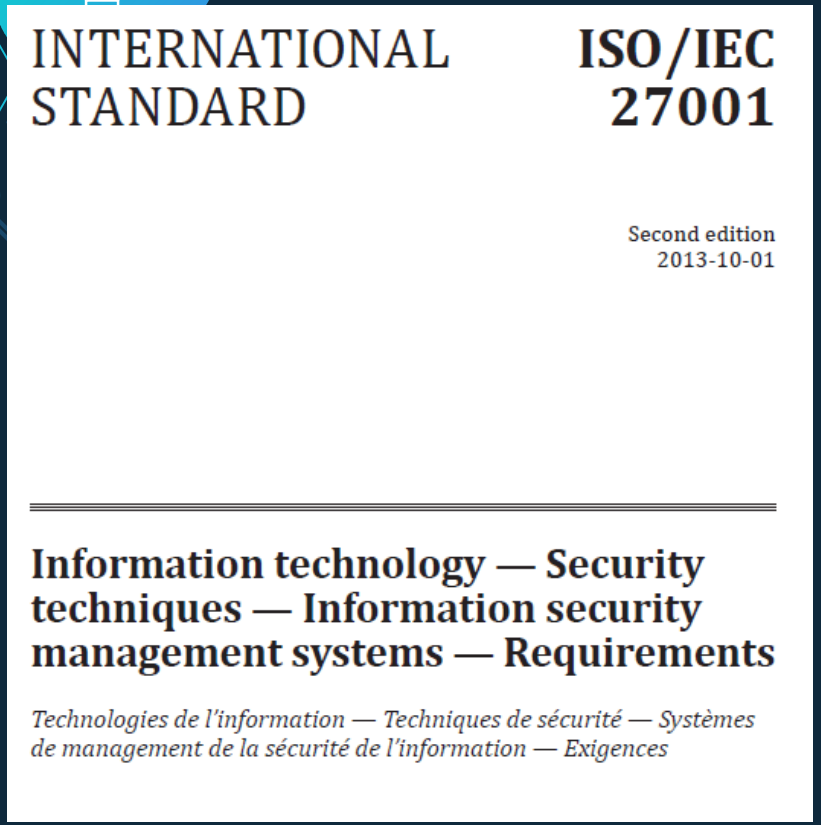
Ingegneri Informatici
Ricercatori
Sistemisti
Programmatori
Esperti di Multimedia e Comunicazione

TRAPANI	MATERA	NAPOLI
Corso Italia, 77	Via Cosenza, 61	Via Cervantes, 55

www.iinformatica.it

iInformatic@ Srls

LA GUIDA CONSIGLIATA



INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

ISO 27000 : Fundamentals and vocabulary

ISO 27001 : ISMS Requirements (normative)

ISO 27002 : ISMS Code of practice (guide)

ISO 27001's Annex A
list of 114 controls /best practices
(35 control objectives, 14 key points from A.5 to A.18)

GDPR

SI APPLICA AL TRATTAMENTO DATI DI CITTADINI EUROPEI

UE 679/2016 – GDPR

Il **General Data Protection Regulation** è il nuovo regolamento europeo per la protezione dei dati che ha l'obiettivo di "fortificare i diritti delle persone fisiche e unificare la Normativa in merito alla protezione dei dati personali all'interno di tutta l'Unione Europea, sostituendo le diverse leggi nazionali presenti nei Paesi Membri", già attivo da Maggio 2016 ma che è entrato definitivamente in vigore dal 25 Maggio 2018.

Art. 5 GDPR

In particolare l’articolo presenta come “il titolare del trattamento è tenuto al rispetto dei principi generali e a **COMPROVARE** la conformità al Regolamento”.
Con “**comprovare**” si intende che il titolare deve avere le prove di adempiere al regolamento, attraverso un documento che esprima in maniera chiara la comprova dell’adeguamento al nuovo trattamento dei dati personali

PRINCIPI

•***Liceità, correttezza e trasparenza*:** i dati devono essere trattati in maniera lecita, corretta e trasparente;

• ***Limitazione delle finalità:*** *le finalità devono essere determinate, esplicite e legittime*; devono essere quindi individuate le finalità in maniera chiara.

• ***Minimizzazione dei dati:*** *i dati devono essere adeguati, pertinenti e limitati*. In merito alla minimizzazione dei dati esiste già un Art. simile (l'Art. 3 del D.lgs 196, il cosiddetto "Principio della necessità")

•***Esattezza:*** *i dati devono essere esatti e, se necessario, aggiornati*. Anche adesso vale lo stesso principio ma con la nuova normativa questo aspetto è stato specificato in modo estremamente chiaro.

• ***Limitazione della conservazione****: i dati devono essere conservati per un periodo temporale limitato al conseguimento delle finalità*. Concetto fondamentale entrato in modo prorompente nei principi del regolamento che obbliga a dare indicazione e motivazione sui tempi di conservazione dei dati.

• ***Integrità e riservatezza****: deve essere garantita un'adeguata sicurezza dei dati personali*

INFORMATIVA

INFORMATIVA

RIFERIMENTO NORMATIVO

CATEGORIE DI DATI E FINALITA’

BASE GIURIDICA DEL TRATTAMENTO
(legge – legittimo interesse – consenso)

TITOLARE DEL TRATTAMENTO (dati identificativi)

DESTINATARI DEI DATI

DURATA DEL TRATTAMENTO

DIRITTI DEGLI INTERESSATI

RESPONSABILE DELLA PROTEZIONE DEI DATI (recapito)

FIGURE DEL GDPR

- *Il Titolare del trattamento;*
- *Il Co-titolare del trattamento;*
- *Il Responsabile del trattamento;*
- *I Soggetti incaricati al trattamento;*
- *Data Protection Officer (DPO)*

TITOLARE DEL TRATTAMENTO

“La persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali”.
È esattamente la stessa definizione espressa nella 196.

ACCOUNTABILITY

OBBLIGHI

-Ha l’obbligo di regolamentazione contrattuale dei ruoli e delle responsabilità per i soggetti coinvolti nel trattamento (co-titolari, responsabili, DPO);
-Nomina di un Data Protection Officer (DPO), se obbligatorio;
-Attuazione di politiche adeguate in materia di protezione dei dati;
-Informativa, privacy da fornire agli interessati e gestione corretta dei consensi;
-Adeguato riscontro ai soggetti interessati che esercitano i propri diritti;
-Rispetto dei principi Privacy by design e Privacy by default;
-Valutazione d’impatto (Impact analysis) ;
-Implementazione di adeguate misure di sicurezza atte a ridurre i rischi;
-Notificazione delle violazioni di dati personali (data breach) all’Autorità e agli interessati;
-Rispetto del principio di Accountability

PRIVACY BY DESIGN AND BY DEFAULT

PRIVACY BY DESIGN

L’azienda nel pianificare un nuovo servizio dovrà chiedersi se in questo nuovo servizio verranno trattati dati personali, e se questi dati sono ordinari o particolari (sensibili).

Se riguarda dati particolari sarà necessario esprimere come verranno tutelati questi dati. Devo quindi, dalla progettazione, fare tutte le valutazioni che riguardano i dati personali qualora essi vengano trattati (DPIA - Valutazione d'impatto sulla protezione dei dati).

DPIA

DPIA (DATA PROTECTION IMPACT ASSESTMENT)

DPIA N. _____ DEL _____
ATTO DI DOCUMENTAZIONE DELLE SCELTE EFFETTUATE

TITOLARE DEL TRATTAMENTO: Il titolare del trattamento è _____

RESPONSABILE DEL TRATTAMENTO: Il responsabile del trattamento è _____

DESCRIZIONE PRODOTTO/PROCESSO/SERVIZIO : Sistema di videosorveglianza così composto : N.3 telecamere interne e N.3 telecamere esterne (sempre attive) con obiettivo adattato alle esigenze del campo di ripresa che riprendono il perimetro aziendale.
Il video server registrerà su HD il flusso video 24h/24h e il personale responsabile del trattamento dovrà cancellare i video ogni 24 ore lavorative.

DESCRIZIONE DEL TRATTAMENTO DATI: Il trattamento dati riguarderà acquisizioni video dalle telecamere distribuite nel perimetro.

VALUTAZIONE DELLA NECESSITA' DEL TRATTAMENTO: L'installazione dell'impianto di videosorveglianza perimetrale non può essere sostituito da nessun altro strumento, posto che non solo può lanciare un allarme in caso di motion detection, cosa che potrebbe essere fatta anche da un impianto di allarme, ma può riprendere con precisione le caratteristiche fisionomiche dell'aggressore e fungere da elemento di deterrenza senza eguali.

FINALITA' PERSEGUITA : Aumento della sicurezza e della protezione dal rischio di rapine nell'azienda.

LEGITTIMO INTERESSE (se applicabile): Il trattamento rientra nella categoria del "legittimo interesse" del titolare del trattamento

MISURE PREVISTE:
L'accesso al videoserver avviene mediante username e password di sicurezza nota al solo titolare e responsabile. Inoltre, l'accesso avviene esclusivamente all'interno della rete intranet o VPN aziendale.

VALUTAZIONE DEL RISCHIO: Basso. La valutazione è determinata dal fatto che i video sono cancellate ogni 24 ore lavorative. Il dispositivo non acquisisce audio e non effettua alcun tipo di elaborazione biometrica. Il sistema è accessibile solo al titolare e responsabile del trattamento mediante password e nella rete locale.

SI ALLEGA STATO DELL'ARTE RIFERIMENTI DEL GARANTE: SI [ ] NO [ ]

E' RICHIESTA LA CONSULTAZIONE PREVENTIVA (PRIOR CHECK) : SI [ ] NO [ ]

Il titolare

Matera_____

_____

DATI PARTICOLARI

Dati sull’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, 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

«ogni dato personale in grado di ledere, anche potenzialmente, la dignità della persona o intaccare senza motivo lecito il suo naturale diritto alla riservatezza»

PRIVACY BY DEFAULT

Il principio di privacy by default stabilisce, invece, che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti.

RESPONSABILE DEL TRATTAMENTO

“Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato“.

RESPONSABILE DEL TRATTAMENTO

-Trattare i dati eseguendo le istruzioni fornite dal titolare;
-Assicurare che le persone autorizzate a trattare i dati personali si siano impegnate a rispettare i vincoli di riservatezza;
-Implementare e mantenere tutte le misure tecniche e organizzative adeguate;
-Rendersi disponibili ad audit di verifica da parte del Titolare del trattamento
-Assistere il titolare del trattamento per la gestione delle richieste di diritto d'accesso e per gli altri obblighi imposti dal Regolamento;
-Fornire al titolare qualsiasi informazione necessaria per dimostrare il rispetto del Regolamento;
-Tenere un registro delle categorie di attività di trattamento dei dati personali svolte per conto del titolare del trattamento;
-Avvertire il titolare del trattamento immediatamente dopo aver riscontrato il verificarsi di una violazione dei dati;
-Cooperare con l'Autorità di Vigilanza;

I SOGGETTI AUTORIZZATI AL TRATTAMENTO

Persone autorizzate dal titolare al trattamento dei dati personali

DPO OBBLIGATORIO

Il DPO è **obbligatorio** nel caso in cui il trattamento dei dati personali sia effettuato:

- da una **pubblica amministrazione** o da un suo organismo
- da aziende ove l'attività principale svolta dal titolare o dal responsabile del trattamento consiste nel trattamento di dati che per la loro natura, oggetto o finalità, richiedono il **controllo regolare e sistematico degli interessati su larga scala**.
- da aziende ove l'attività principale consiste nel trattamento su **larga scala di dati sensibili**, relativi alla salute, alla vita sessuale, genetici, giudiziari e biometrici.

AMMINISTRAZIONE PUBBLICA O SUO ORGANISMO

Per le **amministrazioni e gli enti pubblici** (eccetto le autorità giudiziarie nell'esercizio delle loro funzioni).

Soggetto dotato di personalità giuridica i**stituito per soddisfare specificatamente esigenze di interesse generale**, aventi carattere non industriale o commerciale, soggetto la cui attività sia finanziata in modo maggioritario dallo Stato, dagli enti pubblici territoriali o da altri organismi di diritto pubblico oppure la cui gestione sia soggetta al controllo di questi ultimi oppure il cui organo d'amministrazione, di direzione o di vigilanza sia costituito da membri dei quali più della metà è designata dallo Stato, dagli enti pubblici territoriali o da altri organismi di diritto pubblico.

In particolare il Gruppo Articolo 29 ha raccomandato la nomina del DPO anche per gli organismi privati incaricati dello svolgimento di pubbliche funzioni o che comunque esercitano pubblici poteri (es. forniture elettriche, trasporti pubblici).

Monitoraggio regolare e sistematico di interessati

- la gestione di una rete di telecomunicazioni;
- la prestazione di servizi di telecomunicazioni;
- il reindirizzamento di messaggi di posta elettronica (email retargeting);
- attività di marketing basate sull'analisi dei dati raccolti;
- profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio);
- tracciamento dell'ubicazione, ad esempio da parte di app su dispositivi mobili
- programmi di fidelizzazione;
- pubblicità comportamentale;
- monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili;
- utilizzo di telecamere a circuito chiuso;
- dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, etc.

ESEMPI DI SOGGETTI TENUTI ALLA NOMINA DEL DPO

istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

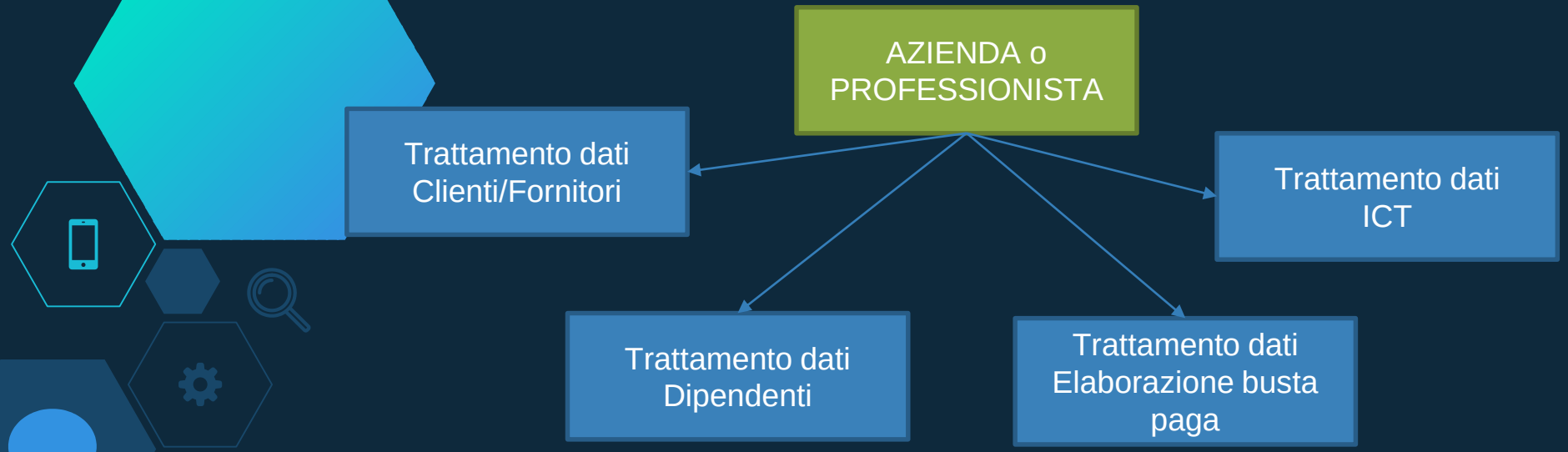
ESEMPI DI SOGGETTI NON TENUTI ALLA NOMINA DEL DPO

In relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.

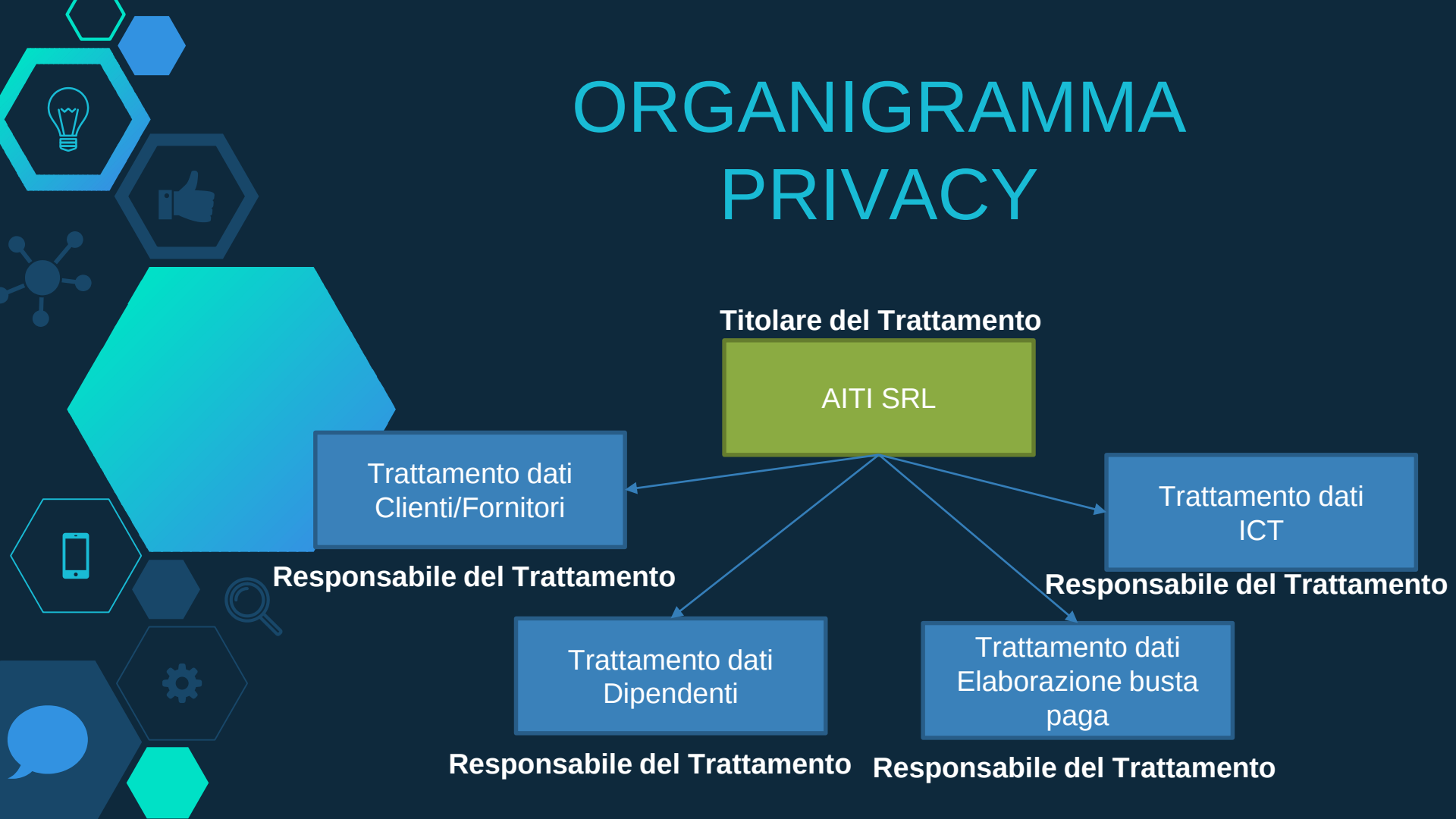
DPO

- Informare e fornire consulenza ai soggetti coinvolti in merito alle attività necessarie volte a garantire la conformità ai requisiti normativi sulla protezione dei dati;
- Esercitare un’azione di controllo e vigilanza per ciò che attiene l’osservanza del Regolamento (politiche interne, attribuzione delle responsabilità, formazione del personale che concorre ai trattamenti, etc.);
- Essere di supporto per la valutazione d’impatto sulla protezione dei dati e monitorare lo svolgimento;
- Essere un punto di contatto per i soggetti interessati, anche in caso di esercizio dei propri diritti, le Autorità di controllo esterne e le funzioni operative e di controllo interne.

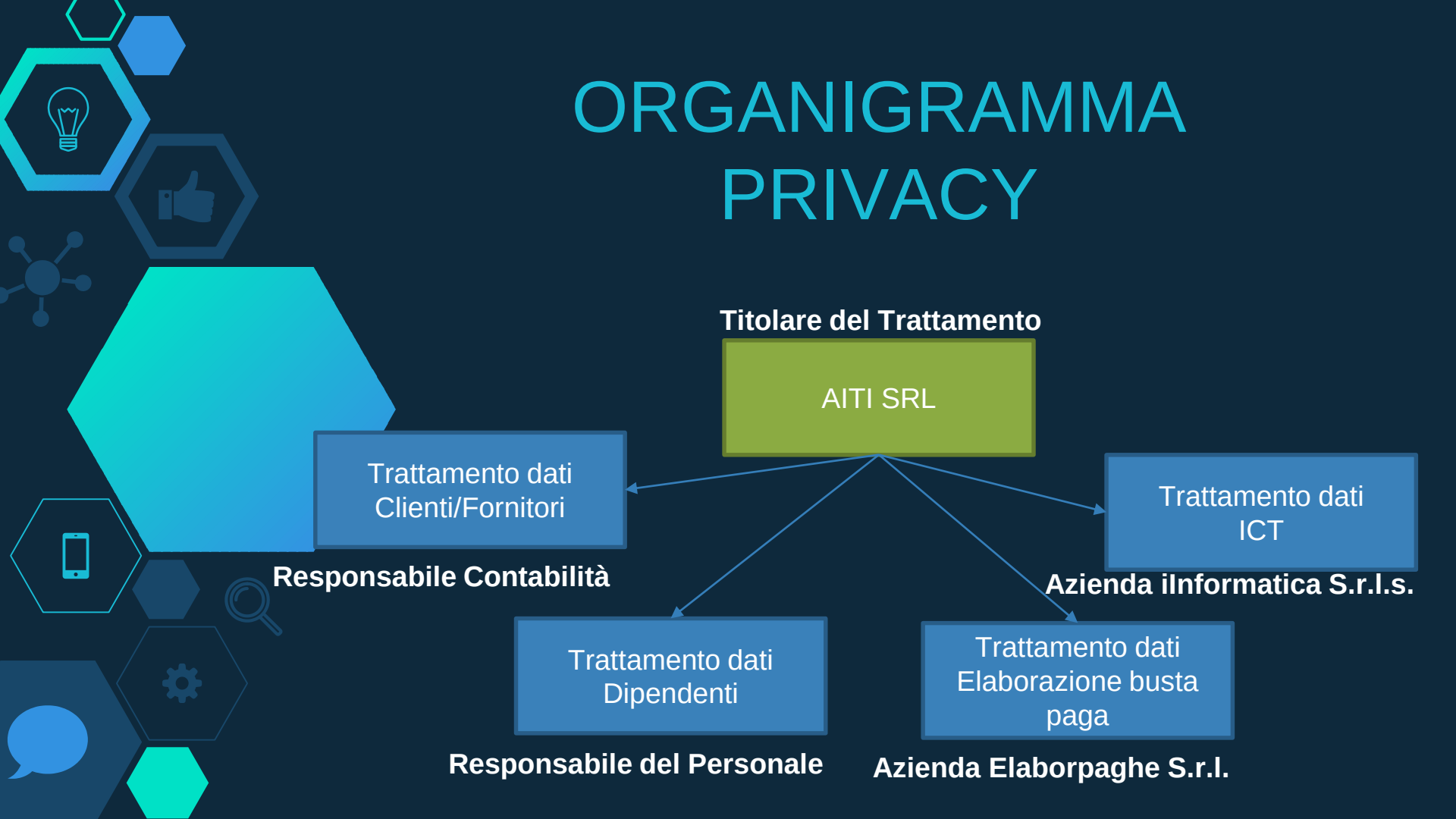
ORGANIGRAMMA PRIVACY



ORGANIGRAMMA PRIVACY



ORGANIGRAMMA PRIVACY



REGISTRO DEL TRATTAMENTO

Sia il titolare che il responsabile del trattamento hanno l’obbligo di tenere un registro delle attività riguardante il trattamento dei dati personali, salvo nel caso in cui l’azienda disponga di un numero di dipendenti inferiore a 250, il trattamento non riguarda dati particolari, giudiziari o non comporta rischi (elementi che devono essere comprovati).

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*

RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERSSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

DATA BREACH

Per “data breach” si intende qualsiasi violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati.

Il data breach, una volta **identificato**, deve essere notificato al garante, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Esempi di data breach

Crash del server
Cryptolocker
Trojan horse
Furto di un harddisk
Furto di un computer

ARTICOLO 32

Sicurezza del trattamento

Il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

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

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

«RID»

RISERVATEZZA – INTEGRITA’ – DISPONIBILITA’

PRINCIPI DELLA SICUREZZA DELLE INFORMAZIONI

- Disponibilità dei dati, ossia salvaguardia del patrimonio informativo nella garanzia di accesso, usabilità e confidenzialità dei dati. Da un punto di vista di gestione della sicurezza significa ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.).
- Integrità dei dati, intesa come garanzia che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.
- Riservatezza informatica cioè gestione della sicurezza in modo tale da mitigare i rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata.

ADEGUATE MISURE DI SICUREZZA

- Asset Licence Management
- Business Continuity
- Disaster Recovery
- Crittografia e profilazione
- Audit di Rete & Penetration Test
- Vulnerability Assestment (IPS, IDS)

Asset Licence Management

Postazione _____

Utente responsabile _____

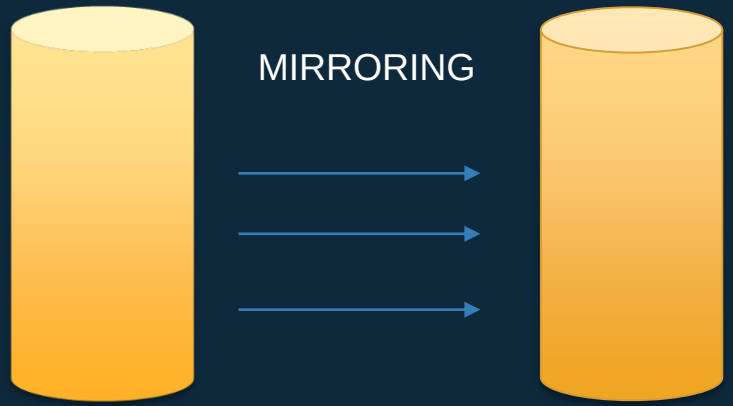
Licenza O.S. _____

Licenza Office_____

Licenza Autocad _____

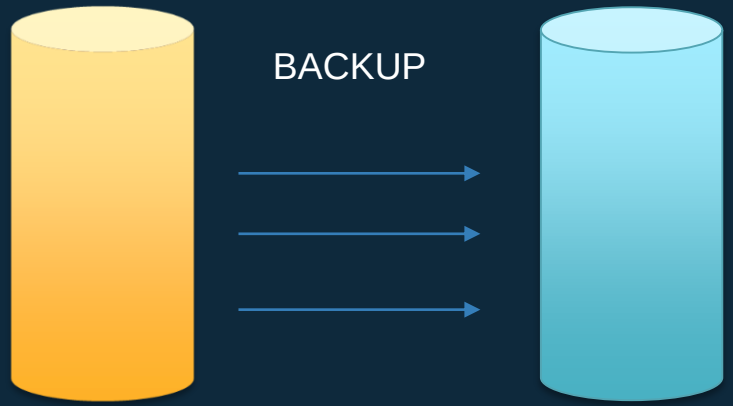
Licenza Antivirus _____

Business Continuity

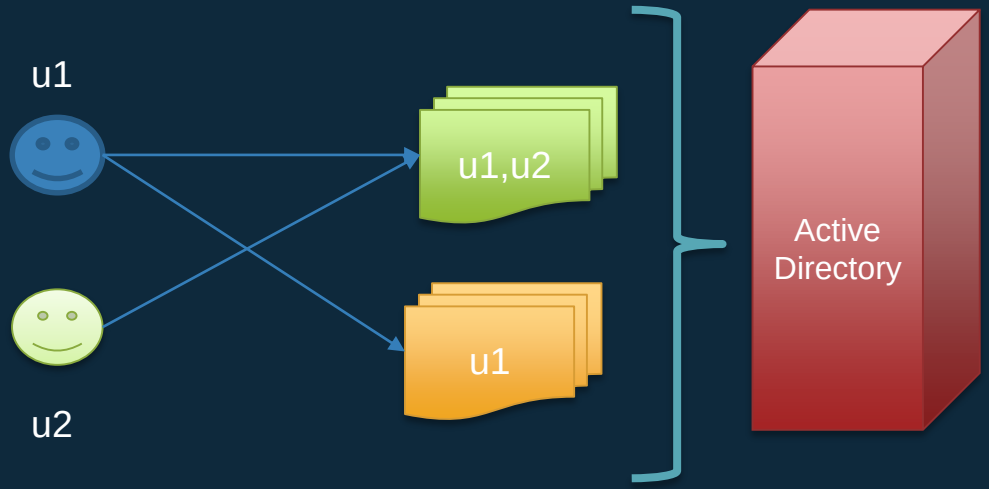


Esempio: RAID

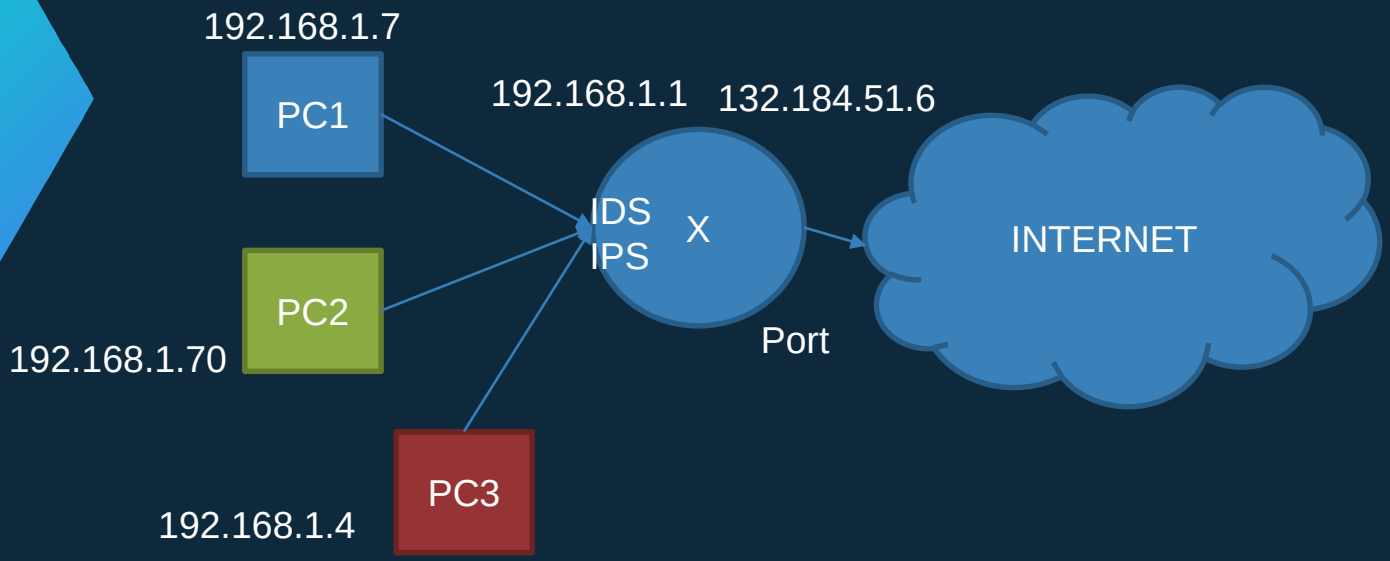
Disaster Recovery



Crittografia e profilazione



Audit di Rete & Penetration Test
Vulnerability Assestment



Best Practices per il professionista

PROFESSIONISTA OPERANTE IN FORMA INDIVIDUALE

◇Non ha obbligo del DPO

◇Non ha obbligo del registro del trattamento (fortemente consigliato)

◇Obbligo DPIA per trattamenti non convenzionali

◇Obbligo di organigramma con nomine

◇Obbligo di informativa clienti/fornitori

◇Obbligo di informativa per dipendenti

◇Obbligo di raccolta consenso «facoltativo» in caso di trattamenti marketing/profilazione

◇Obbligo di registro Databreach

◇Obbligo di misure di sicurezza (Art.32)

Art.32
MISURE PER WEBSITE (FRONT-END)

- **PRESENZA DEL CERTIFICATO SSL**
- **GDPR POLICY (INFORMATIVA) E COOKIE POLICY**
- GESTIONE DEI FORM CON «PRESA VISIONE DELL'INFORMATIVA»
- (CONTATTACI)
- GESTIONE DEI FORM CON «ACQUISIZIONE CONSENSO» (NEWSLETTER/MODULO CV)

N.B. Nella GDPR Policy deve essere indicato il riferimento al RPD se previsto

Art.32
MISURE

- Utilizzo di password robuste per servizi web (es. posta elettronica e pec)
- Accesso profilato a cartelle contenenti dati a rischio violazione GDPR
- Utilizzo di Password su documenti a rischio violazione GDPR (soprattutto se scambiati a mezzo web)
- Antivirus e firewall su singole postazioni (software licenziato)
- Backup dei dati periodico e verificato
- Firewall di rete (utilizzo di VPN per accesso da remoto)

SANZIONI

Le sanzioni applicate in caso di mancato rispetto dei seguenti articoli:

- Art. 5 Violazione dei principi;
- Art. 6 Liceità del trattamento;
- Art. 7 Consenso al trattamento;
- Art. 9 Trattamento di categorie particolari di dati;
- Artt. 12-22 Esercizio diritti degli interessati;
- Art. 13 Informativa;
- Art.. 44-49 trasferimento dati all'estero;

sono pari ad un massimo di 20.000.000 euro o al 4% del fatturato mondiale totale annuo

PER APPROFONDIRE

An innovative approach for the GDPR compliance in Big Data era

Un approccio innovativo per la conformità al regolamento GDPR nell'era dei Big Data

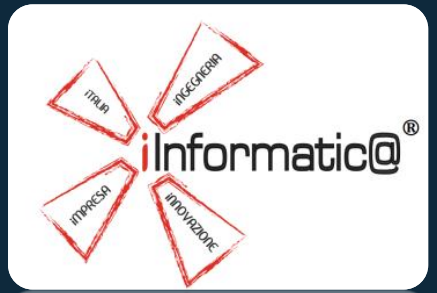
M. Giacalone, C. Cusatelli, F. Fanari, V. Santarcangelo, D.C. Sinitò[1]

Abstract The present work shows a preliminary overview of the Big Data Analytics scenario, introducing the related privacy issues considered by the new General Data Protection Regulation, better known by its acronym GDPR. The work then introduces an innovative index to assess the compliance of a company with this regulation on the protection of personal data, in terms of privacy by design and privacy by default.

Abstract *Il presente lavoro mostra una preventiva panoramica in merito allo scenario del Big Data Analytics, introducendo le relative problematiche di privacy considerate dal nuovo Regolamento Generale sulla Protezione dei Dati, meglio noto con l'acronimo inglese GDPR. Il lavoro introduce quindi un innovativo indice per valutare la conformità di un'azienda a tale regolamento sulla tutela dei dati personali, in termini di privacy by design e privacy by default.*

Key words: GDPR, privacy, Big Data

Thanks!



info@iinformatica.it

www.iinformatica.it