Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 5: Trasferimento Dati Estero e Privacy comparata – controlli ed audit di processo

Unità didattica

M5.1 La circolazione dei dati nelle società multinazionali

Avv. Ida Tascone

La materia del trasferimento dei dati personali all'estero è sempre stata oggetto di grande attenzione in ambito europeo per i suoi inevitabili risvolti in materia di privacy per cui sia la Direttiva comunitaria 95/46/CE che l'attuale Regolamento Europeo n. 2016/679 hanno previsto particolari cautele in tale settore.

In particolare l'art. 44 del GDPR come principio generale sancisce che qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui capo V del Regolamento. Tutte le disposizioni sono applicate al fine di assicurare che il livello di tutela delle persone fisiche garantito dal Regolamento non sia pregiudicato.

Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso, innanzitutto, se la Commissione ha deciso che il paese terzo, o un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscano un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche (art. 45).

In mancanza di una valutazione di adeguatezza il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha offerto garanzie adeguate e a condizione che siano disponibili diritti azionabili degli interessati e mezzi di ricorso effettivi per gli interessati (art. 46).

Il trasferimento dei dati verso paesi terzi può anche avvenire quando vi siano norme vincolanti d'impresa (art. 47) che però devono essere approvate dall'Autorità di controllo purché:
a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo di imprese o gruppi di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;
b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali;
c) soddisfino tutta una serie di requisiti quali l'indicazione della struttura e delle coordinate di contatto del gruppo d'imprese in questione e di ciascuno dei suoi membri; l'indicazione dei trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione; l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione di default, ecc.

Appare quindi evidente che nella materia della tutela dei dati personali vi è da sempre la preoccupazione che, proprio al fine di eludere le protezioni offerte dalle legislazioni degli Stati, i dati personali vengono trasferiti all'estero, verso paesi con una minore, o con nessuna, legislazione sul punto della protezione degli individui rispetto al trattamento dei dati personali.

La stessa Autorità Garante ha sempre sostenuto che per superare gli ostacoli relativi al trasferimento di dati personali presso paesi terzi vengono predisposti su scala europea alcuni contratti-tipo che hanno permesso di regolare in modo uniforme, e tendenzialmente agevole, diversi flussi di dati verso Paesi terzi nei quali operino titolari del trattamento autonomi rispetto al soggetto esportatore, oppure strutture che agiscono in funzione strumentale quali "responsabili" del trattamento.

Il problema è che questo sistema non funziona al meglio per molti gruppi multinazionali in quanto nell'ambito degli stessi l'impiego di modelli contrattuali standardizzati viene avvertito, a volte, come farraginoso, poiché ciascuna società stabilita all'interno dello Spazio economico europeo e appartenente ad un medesimo gruppo multinazionale deve comunque includere le garanzie previste dai predetti schemi tipo in un suo contratto con le società del gruppo situate in Paesi terzi.

Al fine di risolvere tale problematica le autorità garanti d'Europa, riunite nel gruppo istituito ai sensi dell'art. 29 della direttiva 95/46/CE (c.d. Gruppo art. 29), hanno preso in considerazione ulteriori strumenti, rispetto a quello contrattuale, che possano assicurare anch'essi un livello adeguato di protezione per i diritti degli interessati, con particolare riguardo al trasferimento all'estero dei dati personali nell'ambito dei gruppi multinazionali.

Il Gruppo ha operato alcune prime valutazioni con riserva di eventuali situazioni specifiche connesse a singole realtà nazionali, ravvisando un'interessante prospettiva di lavoro nelle regole di comportamento che una società capogruppo può impartire, generalmente all'interno di appositi codici di condotta interni al gruppo multinazionale e resi vincolanti per tutte le società ad esso appartenenti.

Tali regole, ormai conosciute nella prassi applicativa come "*binding corporate rules*", sono state ritenute come uno strumento astrattamente idoneo ad assicurare un livello adeguato di protezione per i diritti degli interessati, compatibile con la disciplina contenuta nella direttiva 95/46/CE sempreché siano vincolanti sia all'interno che all'esterno del gruppo di società.

Esse si concretizzano in un documento contenente una serie di clausole (rules) che fissano i principi vincolanti (binding) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (corporate).

Le Bcr costituiscono un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personali.

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo 5 – Trasferimento dati estero e Privacy comparata – controlli ed audit di processo

Dott. Raffaele Grieco

M5.2 – Privacy Comparata: i tool di analisi delle normative privacy internazionali

Vulnerability assessment

Indagine interna per trovare le debolezze del sistema da tutti i punti di vista (hardware, software, umani)

GDPR

Art. 30 - registro trattamenti

art. 32 - sicurezza

(32.1.d)

art. 35 - valutazione di impatto

art. 42 - certificazione

A che cosa serve

- ad avere un quadro completo della situazione aziendale rispetto alla sicurezza informatica
- conoscere vulnerabilità di vario tipo all'interno dell'azienda, divise per rischio effettivo, localizzazione per aree e probabilità che vengano usate
- a mantenere uno storico degli assessment aziendali

Che cosa si fa

- Catalogare i beni e le risorse del sistema
- Assegnare valori quantificabili di importanza alle risorse
- Identificare le vulnerabilità e minacce potenziali associate a ciascuna risorsa e

  la probabilità che sia attaccata
- (cercare di) eliminare le vulnerabilità più gravi per le risorse di maggior valore – in fretta

2017

WORLD ECONOMIC FORUM

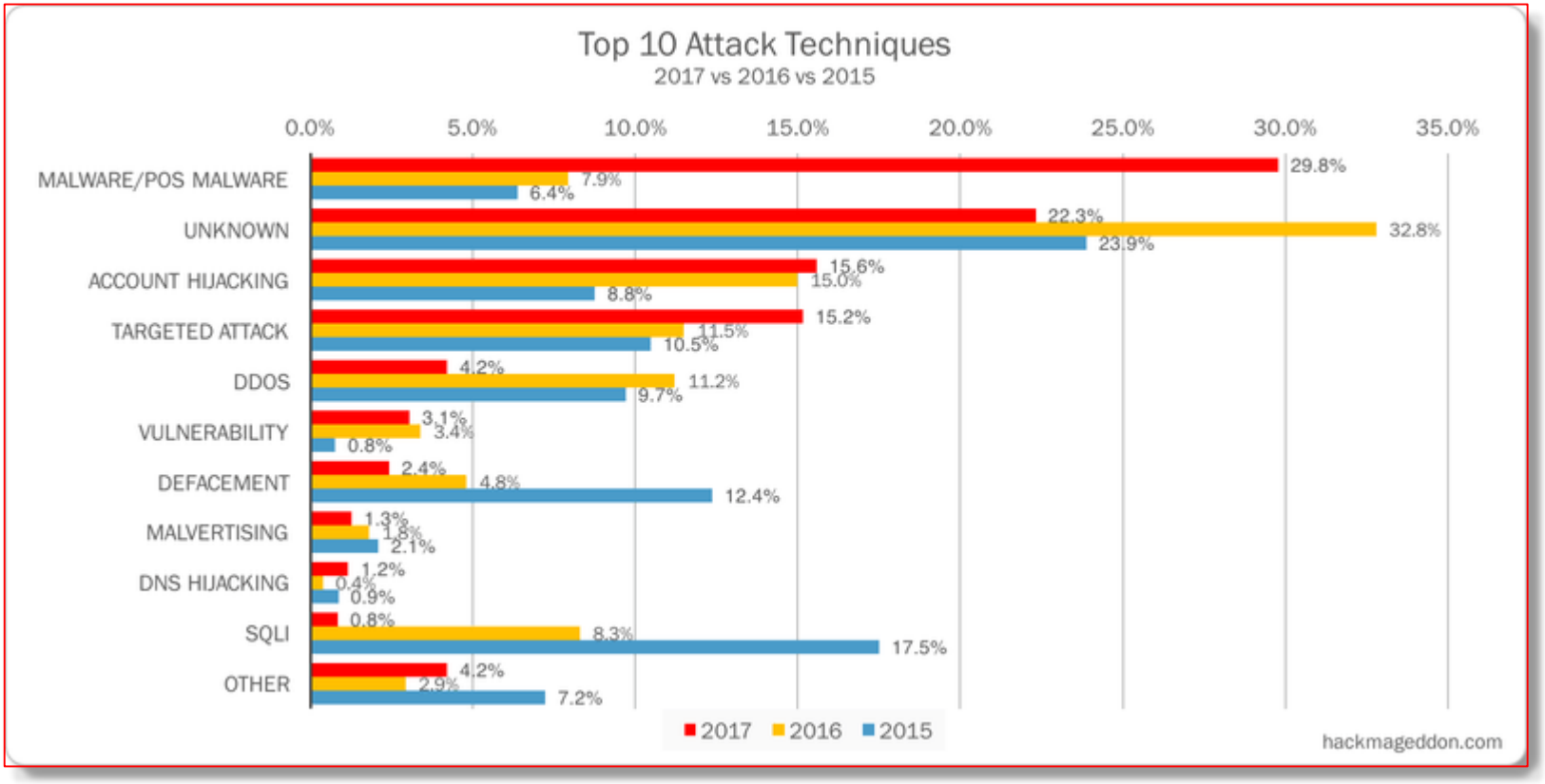
GLOBAL RISKS Report

I top 10 Rischi Probabilità

1. Extreme weather events
2. Natural disasters
3. Cyberattacks
4. Data fraud or theft
5. Failure of climate-change mitigation and adaptation
6. Large-scale involuntary migration
7. Man-made environmental disasters
8. Terrorist attacks
9. Illicit trade
10. Asset bubbles in a major economy

I top 10 Rischi Impatti

1. Weapons of mass destruction
2. Extreme weather events
3. Natural disasters
4. Failure of climate-change mitigation and adaptation
5. Water crises
6. Cyberattacks
7. Food crises
8. Biodiversity loss and ecosystem collapse
9. Large-scale involuntary migration
10. Spread of infectious diseases


Top 10 Attack Techniques
2017 vs 2016 vs 2015
0.0%
5.0%
10.0%
15.0%
20.0%
25.0%
30.0%
35.0%
MALWARE/POS MALWARE
29.8%
7.9%
6.4%
UNKNOWN
22.3%
32.8%
23.9%
ACCOUNT HIJACKING
15.6%
15.0%
8.8%
TARGETED ATTACK
15.2%
11.5%
10.5%
DDOS
4.2%
11.2%
9.7%
VULNERABILITY
3.1%
3.4%
0.8%
DEFACEMENT
2.4%
4.8%
12.4%
MALVERTISING
1.3%
1.8%
2.1%
DNS HIJACKING
1.2%
0.4%
0.9%
SQLI
0.8%
8.3%
17.5%
OTHER
4.2%
2.9%
7.2%
2017
2016
2015
hackmageddon.com

PEN TESTING

Penetration testing

Attacco informatico voluto,
eseguito da persone incaricate ("tiger teams")

...presumibilmente fidate (*'hacker etici'* ?)

PEN TESTING

Serve a cercare le vulnerabilità del sistema, tra cui:

- Porte inutilmente aperte
- Software non aggiornato
- Software con bug noti
- Zero-day
- Problemi hardware (firewall)
- ...

Il pentesting si avvia con la stipula di un contratto che prevede una serie di clausole, condizioni, liberatorie e impegni di discrezionalità

Qualsiasi azione il pentester fa al di fuori del contratto è **illegale.**

Tipi

- Esterno
- Interno
- Blind / double blind

Target

- Applicazioni web
- VPN / VOIP
- Reti wireless
- Accesso remoto
- Risorse umane (social engineering)

Lettura: "come sono riuscita a entrare…"

Informazioni fornite dal cliente

- Teoricamente solo l'IP (o gli IP) – poco efficace in pratica
- Più dati si aggiungono migliore è l'efficacia del test *(gray box)*

Risultato

Un **report** che evidenzia le vulnerabilità trovate nel sistema e le *eventuali* correzioni e modifiche da apportare al sistema

6.8. Indirizzo IP xx.xx.xx.xx

Vulnerabilità	Class.	Soluzione	Note
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32) I cifrari a blocchi obsoleti, aventi una dimensione del blocco di 64 bit, sono vulnerabili a un attacco di collisione se utilizzati in modalità CBC. Sono interessate tutte le versioni dei protocolli SSL/TLS che supportano le suite di crittografia che utilizzano 3DES come cifrario di crittografia simmetrica.	High	Disabilitare il supporto su TLS/SSL per le suite di crittografia che contengono 3DES.	Sulle nuove versioni degli applicativi sono disabilitate di default, pertanto, l'aggiornamento degli applicativi che utilizzano i protocolli TLS/SSL mitigherebbe tale vulnerabilità.
SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST) - (rif. CVE-2011-3389). Vulnerabilità relativa ad una debolezza della crittografia a blocchi (CBC, Cipher Block Chaining) utilizzata nei protocolli SSLv3.0 e TLSv1.0. Potrebbe consentire ad un utente malevolo di carpire informazioni sensibili intercettando il crittografato servito da un sistema	Medium	Inserire una restrizione nell'utilizzo dei soli protocolli TLSv1.1 e TLSv1.2	Nelle ultime versioni dei browser Web è disabilitato di default l'utilizzo del protocollo SSLv3.0.

Il pentesting non può mai essere considerato definitivo

(upgrade, aggiornamenti, cambi di versione, patch...)

I get hired by companies to hack into their systems
and break into their physical facilities to find security holes.
Our success rate is 100%; we've always found a hole.

Kevin Mitnick

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721660021)

NAME: .....MITNICK, KEVIN DAVID

AKA(S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 30/10/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5495
NCIC Fingerprint Classification: ...DOPM20PM13I+PM19PM19

ADDRESS AND LOCALE: KNOWS TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS

software per la
Valutazione di impatto
sulla protezione dei dati

La CNIL, l'Autorità francese per la protezione dei dati, ha messo a disposizione un software di ausilio ai **titolari** in vista della effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA).

www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8581268

Disponibile anche un tutorial in italiano realizzato dal Garante:

www.garanteprivacy.it/regolamentoue/dpia/gestione-del-rischio

Il programma rende eseguibili tutte le operazioni previste dal GDPR, (art. 35, paragrafo 7):

- una **descrizione sistematica** dei trattamenti previsti e delle finalità del trattamento
- una **valutazione** della necessità e proporzionalità dei trattamenti in relazione alle finalità
- una **valutazione dei rischi** per i diritti e le libertà degli interessati
- le **misure** previste per affrontare i rischi

Altri Tool

- l'ICO (la authority britannica) ha pubblicato un **Data protection self assessment toolkit** per aiutare le organizzazioni a valutare il proprio percorso di adeguamento al GDPR.

- il garante spagnolo (AEPD) ha pubblicato un toolkit di *GDPR self-assessment* chiamato **Facilitates RGPD** (riservato a chi non esegua trattamenti a rischio elevato assoggettabili a DPIA).

ASMEFORM
ENTE DI FORMAZIONE

Certificato di Qualità N.2649
ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO
Norma: UNI EN ISO 9001:2008
SGQ - Settore: 37

Corso di Formazione Manageriale Responsabile protezione dei dati "DPO" UE 2016/679

Modulo V Trasferimento Dati Estero e Privacy comparata – controlli ed audit di processo

M5.3 Integrazione degli adempimenti privacy con il sistema qualità

Unità didattiche

M5.3.1 Il principio PDCA: trasformare gli adempimenti in processi di gestione
M5.3.2 Elementi comuni al sistema qualità e quello di gestione della privacy
M5.3.3 I processi di controllo di un sistema di gestione della privacy
M5.3.4 Il "mantenimento e la sorveglianza del sistema da parte del DPO

Ing. Salvatore Minucci

M5.3 Integrazione degli adempimenti privacy con il sistema qualità

- M5.3.3.1
  - *Il modello PDCA: trasformare gli adempimenti in processi di gestione.*
- M5.3.2
  - *Elementi comuni al sistema qualità e quello di gestione della privacy.*
- M5.3.3
  - *I processi di controllo di un sistema di gestione della privacy.*
- M5.3.4
  - *Il mantenimento e la sorveglianza del sistema da parte del DPO.*

- **M5.3.1**

Il modello PDCA: trasformare gli adempimenti in processi di gestione.

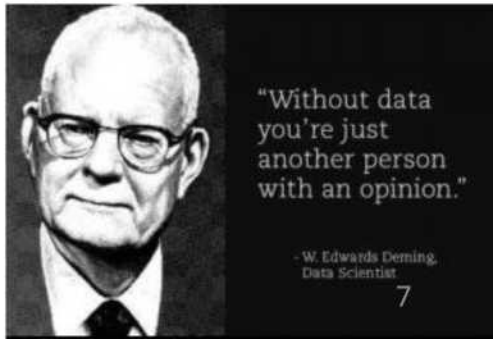
SISTEMA DI GESTIONE

- modello organizzativo implementato mediante l'applicazione organica e sistematica di regole e procedure, a tutti i livelli dell'organizzazione, allo scopo di raggiungere uno specifico obiet[4-1"']

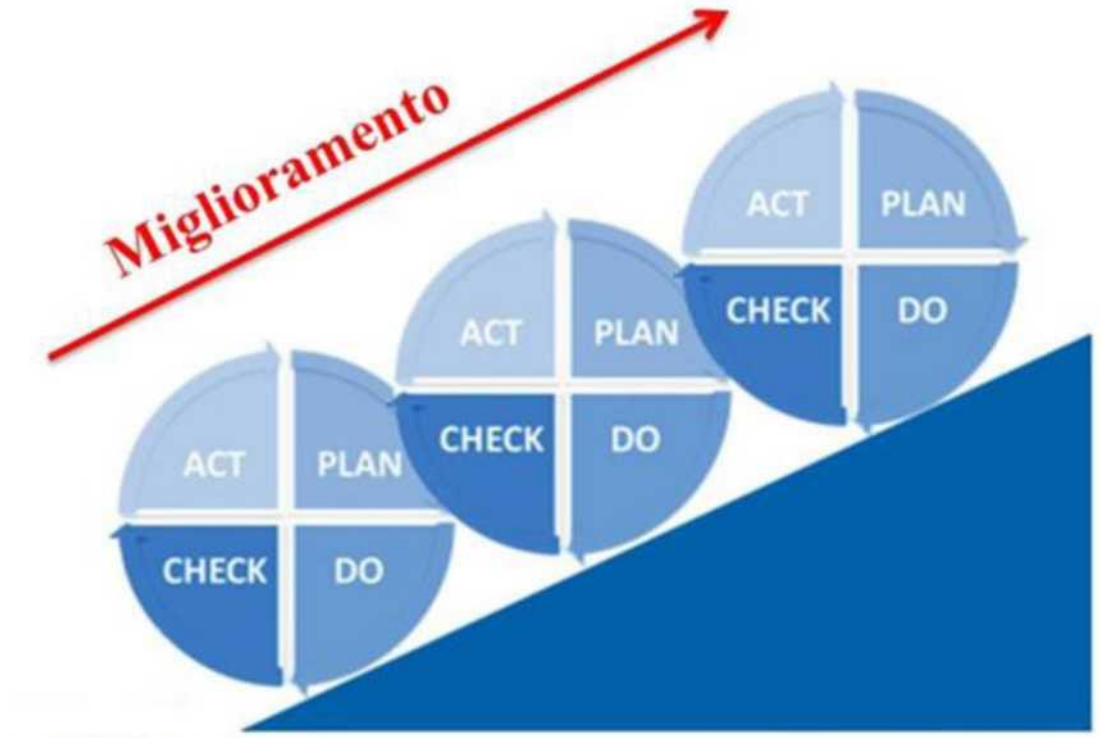
- insieme di regole (documentate e non)
- Insieme di sistemi informatici
- insieme di risorse

- Un sistema di gestione si applica sulla base di un principio semplice: la coerenza.
  - dire quello che si vuole fare e come si vuole farlo
  - attuare quello che si è detto di fare
  - registrare quello che è accaduto
  - **controllare e dare evidenza di quanto fatto**
  - trarre insegnamento dai propri errori
  - cercare continuamente di migliorare

Questi principi semplici sono racchiusi nel modello PDCA, applicabile all'intero sistema, ma anche alle singole attività



- Il modello PDCA è la base del miglioramento continuo



PLAN (Pianificare)

- stabilire gli obiettivi
- definire i processi e le azioni necessari
- definire le risorse
- assegnare ruoli e responsabilità
- stabilire gli indicatori di performance

- DO (Fare)

  - Attuare quanto pianificato

CHECK (Controllare)

- Raccolta dei risultati
- Confronto con gli obiettivi
- Verifica del rispetto delle regole
- Analisi degli inconvenienti o degli effetti collaterali
- Analisi delle opportunità

- ACT (agire)
  - Definire azioni migliorative
  - Definire azioni correttive
  - Modificare i processi

- **M5.3.2**

Elementi comuni al sistema qualità e quello di gestione della privacy.

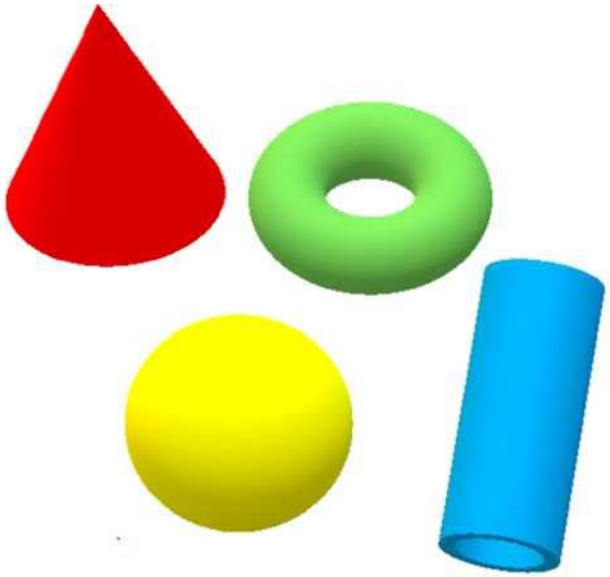
- GDPR e ISO 9001
  - Applicare il GDPR significa far entrare neN'operatività quotidiana anche la gestione dei dati personali.
  - L'applicazione efficace del GDPR non è un atto burocratico, formalmente perfetto ma inapplicato nella realtà, ma deve inquadrarsi come un processo vero e proprio, volto alla gestione reale dell'azienda ed al suo miglioramento.
  - Questo concetto è lo stesso che si attua nei Sistemi di Gestione per la Qualità (UNI EN ISO 9001:2015).

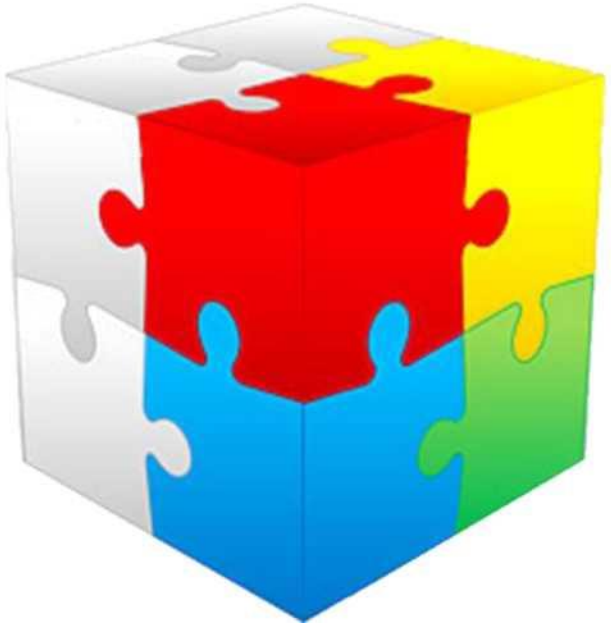
- Il Sistema di Gestione Qualità **ISO 9001** è uno standard volontario che definisce i **requisiti** che un'organizzazione deve avere per:
  - dimostrare la propria capacità di fornire con **regolarità** prodotti e/o servizi che soddisfino i requisiti del cliente e **cogenti**;
  - Migliorare in modo continuo

- Il Regolamento **GDPR** è una norma cogente che definisce i **requisiti** minimi che un organizzazione deve avere per:
  - dimostrare la protezione delle persone fisiche con riguardo al trattamento dei dati personali.

- La presenza di un SGQ permette di introdurre il GDPR in modo integrato nel sistema generale di gestione dell'organizzazione (Azienda o Ente).

- L'integrazione dei vari aspetti della gestione di un'organizzazione (Azienda o Ente), consente una visione organica del Sistema, ed è la base di una gestione globale efficace ed efficiente.





Punti di contatto tra UNI EN ISO 9001 ed il GDPR

- L'organizzazione deve mettere a disposizione **le <u>persone</u> <u>necessarie</u>** per l'attuazione del SGQ (par. 7.1.2 della norma ISO 9001), quindi, se rientra nei casi previsti dal Regolamento Europeo Privacy, anche un DPO.

Punti di contatto tra UNI EN ISO 9001 ed il GDPR

- L'organizzazione deve mettere a disposizione **l'infrastruttura necessaria** per l'attuazione del SGQ (par. 7.1.3 della norma ISO 9001), quindi, anche sistemi HW e SW, Antivirus, Back Up, Disaster Recovery Plan.

Punti di contatto tra UNI EN ISO 9001 ed il GDPR

- L'organizzazione deve assicurare che le **persone siano competenti** ed eventualmente deve formarle (par. 7.2 della norma ISO 9001).

- Il che significa che, se occorre, dovrà formare il DPO. Ma non solo, la formazione ha un ruolo fondamentale in generale per tutte le risorse umane, e all'interno dello stesso GDPR è prevista una formazione obbligatoria.

Punti di contatto tra UNI EN ISO 9001 ed il GDPR

- L'organizzazione deve assicurare che **le persone siano consapevoli** del proprio contributo all'efficacia del SGQ, compresi i benefici derivanti dal miglioramento delle prestazioni (par. 7.3 della norma ISO 9001).

- Il che significa che all'atto di una nuova assunzione, o di un cambio di mansione, si dovrà rendere consapevole la persona stessa dell'importanza della corretta gestione del trattamento dei dati personali.

Punti di contatto tra UNI EN ISO 9001 ed il GDPR

- L'organizzazione deve assicurare che i processi, prodotti e **servizi forniti dall'esterno** non influenzino negativamente la capacità dell'organizzazione di rilasciare con regolarità ai propri clienti, prodotti e servizi conformi (par. 8.4.2 della ISO 9001): in base alla tipologia di servizio reso da un fornitore, potrebbe esserci la necessità di nominarlo responsabile esterno del trattamento dati oppure amministratore di sistema.

Punti di contatto tra UNI EN ISO 9001 ed il GDPR

- L'organizzazione deve aver cura della **proprietà dei clienti** (par. 8.5.3 della ISO 9001): per proprietà dei clienti si intendono anche i dati personali.
- L'organizzazione deve quindi dichiarare come utilizza i dati personali, come li conserva e li protegge, come li recupera se sono conservati su supporti informatici.

Punti di contatto tra UNI EN ISO 9001 ed il GDPR

- Integrare all'interno di un SGQ esistente anche la gestione dei dati personali è un concreto vantaggio perché, possiamo contare su una struttura gestionale già collaudata e nota all'organizzazione.

  - modalità di gestione già note
  - gestione documentale controllata
  - attività di revisione e di audit

- **M5.3.3**

  I processi di controllo di un sistema di gestione della privacy.

- Tutte le attività fondamentali di un DPO trovano riscontro nei requisiti della ISO 9001:2015 relativa ai Sistemi di Gestione per la Qualità:
  - Conoscere tutti gli aspetti organizzativi dell'azienda
  - Individuare un organigramma privacy e prevedere un coordinamento funzionale
  - Mappare e classificare i trattamenti
  - Prevedere specifiche policy del trattamento dei dati

- Attività fondamentali di un DPO
  - Analizzare l'impatto delle nuove tecnologie in ambito protezione dei dati
  - Aiutare il titolare del trattamento nel predisporre un'efficace politica di sicurezza
  - Curare, tramite il titolare del trattamento, i rapporti con gli interessati
  - Supportare il titolare del trattamento nella predisposizione di specifici report di data breach

- Attività fondamentali di un DPO
  - Aiutare il titolare del trattamento nella predisposizione e gestione di specifici audit privacy interni ed esterni
  - Mantenersi aggiornati con riferimento alla normativa nazionale ed europea
  - Curare i rapporti con l'Autorità garante su tutte le tematiche che dovessero investire l'azienda o l'ente in materia di privacy
  - **Monitorare in generale tutte le attività di trattamento dati al fine di assicurare il rispetto della normativa**

- **M5.3.4**

  Il mantenimento e la sorveglianza del sistema da parte del DPO.

- (WP29) Compito fondamentale del DPO è di Vigilare sull'osservanza del Regolamento (art 39, paragrafo 1, lettera b) attraverso un monitoraggio (audit) regolare e sistematico.

- (WP29) REGOLARE
  - che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
  - ricorrente o ripetuto a intervalli costanti;
  - che avviene in modo costante o a intervalli periodici

- (WP29) SISTEMATICO
  - Approccio per sistemi
  - predeterminato, organizzato o metodico;
  - include almeno:
    - Un approccio basato sull'analisi dei rischi
    - l'analisi e la verifica dei trattamenti svolti
    - un processo di raccolta di dati
    - l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo V

Ing. Salvatore Minucci

ARGOMENTO 4

L'ATTIVITÀ DI AUDIT SECONDO LA NORMA ISO 19011 APPLICATA AL GDPR

- M5.4.1
  - *Definizione e tipologie di audit e normative di riferimento*
- M5.4.2
  - *Ruoli e competenze dell'auditor*
- M5.4.3
  - *Pianificazione: programmi, piani, fasi, aree critiche, tool di supporto*
- M5.4.4
  - *Conduzione degli audit, Risultati e rapporti dell'audit*

- **M5.4.1**

  Definizione e tipologie di audit e normative di riferimento.

Scopo di un Audit

- Valutare se i vari elementi di un sistema di gestione sono attuati ed idonei a conseguire l'obiettivo della protezione dei dati personali sulla base dei requisiti del GDPR.
  - Si può paragonare ad un check up effettuato dall'auditor (il medico) che ove riscontri qualcosa che non va (patologia) richiede o definisce opportune azioni correttive (cura).

AUDIT e GDPR

- Nella versione inglese il termine AUDIT è utilizzato 4 volte, nella versione italiana è sostituito dai termini revisione, controllo e verifica.
- Il termine inglese Audit richiede però attività più complesse e strutturate di un semplice controllo.

Ruoli

- CHI RICHIEDE UN AUDIT
  - **COMMITTENTE**: organizzazione o persona che richiede l'audit.

- CHI ESEGUE
  - **GRUPPO DI VERIFICA**: uno o più valutatori che eseguono l'audit
  - **VALUTATORE**: persona che ha la competenza per effettuare l'audit
  - **ESPERTO TECNICO**: persona che fornisce competenze specifiche sull'oggetto dell'audit

Criteri, Evidenze e Risultanze

- RISPETTO A COSA CONDURRE LA VALUTAZIONE
  - **CRITERI** della verifica ispettiva (nel nostro ambito i requisiti del GDPR e le procedure definite dall'organizzazione)

- COSA CERCARE
  - **EVIDENZE**: registrazioni, dichiarazioni di fatto o altre informazioni che sono identificabili e pertinenti ai criteri.

- IL GIUDIZIO
  - **RISULTANZE**: risultati della valutazione delle evidenze della rispetto ai criteri (in genere si esprime come una conformità, non conformità o osservazioni)

Tipologie di Audit

- **Audit di Prima Parte** (autocontrollo)
  - Eseguite da un'organizzazione sulla attuazione e sull'efficacia del proprio sistema o di sue.

- **Audit di Seconda Parte** (su di un partner)
  - Eseguite da un'organizzazione su propri fornitori o subfornitori. (es. su fornitori di servizi IT, su consulenti del lavoro…)

Tipologie di Audit

- **Audit di Terza Parte** (Controllo indipendente)
  - Un'organizzazione effettua la valutazione del sistema di un ente terzo indipendente al fine di certificarne la conformità.
  - E' la modalità usuale con cui vengono condotti gli audit ai fini della **CERTIFICAZIONE**
    - » Certificazione: cenni nel seguito…

Linee guida per la conduzione di audit

- La ISO 19011:2018
  - linea guida per audit di sistemi di gestione
  - si applica indipendentemente
    - dallo scopo del sistema di gestione
    - dalle dimensioni dell'organizzazione
    - dall'attività svolta

Linee guida per la conduzione di audit

- La ISO 19011:2018; è una guida:
  - sui principi dell'attività di audit
  - sulla gestione dei programmi di audit
  - sulla conduzione degli audit di sistemi di gestione
  - sulla competenze delle persone coinvolte nel processo di audit.

Linee guida per la conduzione di audit

- La ISO 19011:2018 è applicabile a qualsiasi organizzazione che abbia l'esigenza di pianificare e condurre audit interni o esterni di sistemi di gestione o di gestire un programma di audit.

CERTIFICAZIONE

- Le certificazioni attestano il rispetto dei requisiti previsti dalle norme e dagli standard internazionali riguardo la conformità di prodotti, servizi, processi, sistemi e persone.

- Sono rilasciate da un organismo di parte terza accreditato, indipendente.

- L'indipendenza è verificata e attestata dall'Ente di accreditamento (in Italia ACCREDIA).

CERTIFICAZIONE e GDPR

- Art. 5.2 - il principio di responsabilizzazione
  - Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

- Art 24 - Responsabilità del titolare del trattamento
  - L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

CERTIFICAZIONE e GDPR

- Gli artt. 42 e 43 del Regolamento danno ampio spazio alla certificazione ed agli organismi di certificazione.

- In particolare l'art. 42 prevede che gli Stati membri, le autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggiano, in particolare a livello di Unione, **l'istituzione di meccanismi di certificazione** della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al Regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento.

CERTIFICAZIONE e GDPR

- Accredia, ha avviato le attività di accreditamento in ambito privacy, su base volontaria, qualificando due schemi di certificazione proprietari (**ISDP 10003 e SGCMF 10002** di cui l'organismo di certificazione INVEO è lo scheme owner).

- Una certificazione già attiva in materia di protezione dei dati personali è anche quella conforme alla norma **ISO/IEC 27001, che riguarda i sistemi di gestione per la sicurezza delle informazioni**, integrata con le linee guida ISO/IEC 27018 per la gestione del cloud.

CERTIFICAZIONE e GDPR

- La certificazione non è esimente
  - (art. 42.3) la certificazione […] non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti […]

- **M5.4.2**

  Ruoli e competenze dell'auditor.


Conoscenze e Competenze Specifiche GDPR
Conoscenze e Competenze generali
Istruzione
Esperienze di lavoro
Formazione come Auditor
Esperienze di Audit
Caratteristiche Personali

Caratteristiche personali

- apertura mentale
- maturità
- capacità di giudizio
- abilità analitica
- tenacia
- obiettività
- onestà (intellettuale)
- diplomazia e tatto
- capacità di sintesi
- capacità di comunicazione
- capacità di lavorare in gruppo
- curiosità professionale.

Caratteristiche personali

- Tali caratteristiche permettono di condurre una verifica :
  - senza pregiudizi;
  - evitando atteggiamenti polemici, ironici, autoritari
  - con sensibilità e rispetto dell'interlocutore e dell'operato altrui
  - reagendo efficacemente in situazioni di tensione
  - raccogliendo elementi basandosi solo su evidenze oggettive e dati di fatto
  - rimanendo fermo nelle conclusioni raggiunte anche in presenza di sollecitazioni a cambiarle

Conoscenze e Competenze Generali

- Principi, procedure e tecniche di audit
  - per mettere in grado l'auditor di applicare quelli appropriati ai diversi audit ed assicurare che gli audit stessi siano eseguiti in modo sistematico e coerente.
- Sistema di gestione e documenti di riferimento
  - per consentire all'auditor di comprendere il campo dell'audit e di applicarne i criteri
- Situazioni organizzative
  - per consentire all'auditor di comprendere il contesto operativo dell'organizzazione.
- Le leggi applicabili, i regolamenti ed altri requisiti attinenti alla disciplina
  - per consentire all'auditor di svolgere la propria attività e di essere consapevole dei requisiti che si applicano all'organizzazione oggetto dell'audit.

Grado di istruzione

- Gli Auditor dovrebbero aver conseguito un grado di istruzione sufficiente a consentirgli di acquisire le conoscenze e le competenze descritte

Esperienza di Lavoro

- Gli Auditor dovrebbero avere esperienza di lavoro che contribuisca allo sviluppo delle conoscenze e delle competenze.
- L'esperienza di lavoro dovrebbe essere maturata in una posizione tecnica, gestionale o professionale che abbia comportato l'esercizio nella capacità di giudizio, nella soluzione di problemi e nella comunicazione con altro personale avente incarichi gestionali o professionali, con persone di pari livello, con clienti e/o con altre parti interessate.

Esperienza di Lavoro

- L'esperienza di lavoro, almeno in parte,
  - dovrebbe essere maturata in una posizione nella quale le attività svolte contribuiscano allo sviluppo delle conoscenze e delle competenze nel campo della gestione della privacy.
  - dovrebbe comprendere la formazione e l'addestramento come auditor che contribuisca allo sviluppo delle conoscenze e delle competenze
  - dovrebbe comprendere l'esperienza di audit. Questa esperienza dovrebbe essere maturata sotto la direzione e la guida di un auditor che abbia le competenze di responsabile di gruppo di audit.

L'atteggiamento

- Il valutatore deve dimostrare serenità ed equilibrio, senza preoccuparsi di risultare necessariamente "simpatico" agli interlocutori, rimanendo concentrato sull'oggetto della verifica.

- Un atteggiamento risoluto e cordiale, rispettoso ma non remissivo, collaborativo ma non "consulenziale", e soprattutto una costante attenzione a distinguere le sensazioni personali dagli elementi oggettivi.

L'atteggiamento

- Ecco alcuni suggerimenti pratici:
  - chiarire che le annotazioni sul diario non sono necessariamente NC
  - di fronte ad azioni volte a far perdere tempo, ricondurre la VI all'alveo originale
  - chiarire i motivi per cui si pone una domanda
  - contenere i tempi di pausa
  - di fronte a stati emotivi particolari, allentare momentaneamente la "presa"
  - non saltare subito alle conclusioni
  - mostrare un pizzico di "ingenuità"
  - evitare domande "autorispondenti"
  - evitare posizioni di eccessivo rigore o lassismo, agevolate dai rapporti preesistenti
  - non stendere un'opinione a ciò che non è stato ancora visto
  - non assumere atteggiamenti "didattici" o del tipo "up-down"

La Comunicazione

- Una comunicazione poco efficace può generare gli stessi effetti di un clima conflittuale e privare di efficacia la verifica stessa.
- Qualsiasi tipo di comportamento è comunicazione, quindi si può affermare che anche il silenzio è comunicazione.
- Ogni forma di comunicazione determina un tipo di risposta da parte dell'interlocutore.

La comunicazione

- Oltre al contenuto, noi comunichiamo qualcosa anche attraverso i cosiddetti "messaggi non verbali":
  - volume, timbro
  - ritmo
  - postura
  - gestualità

La Comunicazione

- Prima ancora del contenuto, è il MODO con cui comunichiamo ad essere recepito a livello inconscio dal nostro interlocutore e a produrre in lui una determinata risposta.
- L'ascolto costituisce il 50% della comunicazione tra due individui.
- Una comunicazione è efficace solo se l'"emittente" e il "ricevente" attuano una formula di ascolto attivo.

- **M5.4.3**

  Pianificazione: programmi, piani, fasi, aree critiche, tool di supporto.

LE FASI DI UNA VERIFICA ISPETTIVA

- Le fasi della VI
  - Pianificazione
  - Conduzione
  - La verbalizzazione (report)

LE FASI DI UNA VERIFICA ISPETTIVA

- Pianificazione
  - Raccolta dei dati di ingresso
  - Predisposizione dei documenti di lavoro
  - Formazione del gruppo
  - Redazione del programma

LE FASI DI UNA VERIFICA ISPETTIVA

- CONDUZIONE
  - Riunione iniziale (riunione di apertura)
  - Impostazione fase esecutiva
  - Osservazioni su come procede il lavoro
  - Valutazione delle attrezzature, risorse, impianti
  - Discussioni e interviste con il personale
  - Dichiarazione dei rilievi
  - Le richieste di azioni correttive (RAC)
  - Riunione di chiusura

LE FASI DI UNA VERIFICA ISPETTIVA

- LA VERBALIZZAZIONE
  - La redazione del rapporto
  - Le azioni successive alla Verifica Ispettiva

LA PIANIFICAZIONE

- Pianificazione
  - definizione dello scopo e dell'estensione della VI
  - Raccolta informazioni ed esame della documentazione di riferimento
  - redazione lista di controllo
  - identificazione delle risorse necessarie

LA PIANIFICAZIONE

- La definizione dello scopo (conformità, efficacia) e dell'estensione (quali aree, elementi del SGQ da sottoporre a verifica) sono attività che spettano al Committente, così come la scelta del Responsabile del Gruppo di Verifica (RGVI).
- Il RGVI ha il compito di raccogliere ed analizzare la documentazione di riferimento.
- Ciò allo scopo di:
  - valutarne la conformità e l'adeguatezza
  - redigere la lista di riscontro

LA PIANIFICAZIONE

- L'esame della documentazione (Procedure, Istruzioni) premette di conoscere con adeguato livello di dettaglio il modo con cui vengono condotte le varie attività.
- La lista di riscontro è un documento fondamentale per la conduzione della VI. Essa è lo strumento che permette di verificare in modo completo il rispetto delle regole stabilite.
- Inoltre, il suo uso riduce il livello di "incertezza" legato alla verifica.

LA PIANIFICAZIONE

- Per una maggiore efficacia della VI, è necessario che la lista di riscontro contenga quesiti derivati direttamente dalla documentazione applicabile.
- Essa serve anche a stimare la possibile durata della Verifica.
- Il RGVI, sulla base delle informazioni attinte, identifica le risorse necessarie e, eventualmente, seleziona i membri del gruppo (AVI).

LA PIANIFICAZIONE

- Sia il RGVI che gli AVI devono rispondere a requisiti di:
  - indipendenza
  - addestramento
  - competenza tecnica
  - compatibilità
- Possono far parte del GVI anche Esperti Tecnici od osservatori esterni

DOCUMENTAZIONE DI SUPPORTO

- *Procedura della VI*
- Programma della verifica
- Istruzioni
- Lista di riscontro

IL PROGRAMMA

- La redazione del programma di visita è l'attività che conclude la pianificazione.
- Esso dovrebbe includere almeno:
  - obiettivi ed estensione della VI
  - componenti del gruppo di VI e ruoli
  - indicazione dei documenti di riferimento
  - data e luogo in cui la VI sarà eseguita
  - le funzioni, siti, attività da verificare
  - riferimenti al metodo di verifica da seguire
  - Orari e durata di ciascuna attività della VI
  - data e ora delle riunioni di apertura/chiusura

IL PROGRAMMA

- Il programma va trasmesso con un certo anticipo al Responsabile dell'area interessata.
- Dovrebbe essere fornita ogni informazione riguardo a:
  - personale che si desidera convocare
  - aspetti logistici
  - metodo della verifica
  - Il metodo di verifica si basa su di un principio di campionamento casuale.

ISTRUZIONI

- Sono una descrizione delle operazioni da svolgere nel corso dell'indagine con un dettaglio più o meno spinto a seconda dell'autonomia che si vuole lasciare ai singoli componenti del gruppo.

LISTA DI RISCONTRO

- La lista di riscontro è un ulteriore importante strumento nella conduzione della verifica ispettiva.
- La lista di riscontro non è altro che la trasposizione in forma interrogativa delle disposizioni previste dalla documentazione di riferimento.
- E' opportuno che la lista di riscontro sia il più possibile aderente alla realtà operativa dell'area che si sta valutando.

LISTA DI RISCONTRO

- è la linea guida dell'esecuzione della VI
- consente di non improvvisare
- riduce l'aleatorietà
- riduce le personalizzazioni
- evita le dimenticanze
- riferita a prescrizioni applicabili
- formulata in modo semplice e chiaro

LISTA DI RISCONTRO

- formulata in modo non generico
- rendere semplice la risposta e la verifica
- corredata da appunti o note per le azioni da svolgere
- formulata secondo una sequenza logica
- un solo quesito in ogni domanda
- pesata
- coprire tutti i temi trattati dalla documentazione

- **M5.4.4**

  Conduzione degli audit, Risultati e rapporti dell'audit.

LA CONDUZIONE

- Riunione di apertura
  - Incontro fra i valutatori e i rappresentanti dell'organizzazione sottoposta a verifica.
- Argomenti trattati nella riunione di apertura:
  - introduzione
  - elenco dei partecipanti
  - elenco dei valutatori
  - sede degli incontri e organizzazione logistica
  - obiettivi della valutazione
  - norme di riferimento

LA CONDUZIONE

- individuazione del personale delegato
- spiegazione dei metodi di valutazione
- programma temporale della verifica
- programmazione della riunione finale
- modalità di elaborazione del rapporto
- modalità di risposta al rapporto
- procedure per le azioni correttive
- garanzia di riservatezza

LA CONDUZIONE

- La preparazione della VI richiede quindi di:
  - focalizzare l'attenzione sugli obiettivi della VI
  - focalizzare l'attenzione sulle prescrizioni che il SG deve rispettare e attuare
  - informare i valutatori dei risultati di eventuali VI precedenti se ve ne sono state
  - ridurre il carico di lavoro del valutatore durante la fase investigativa

LA CONDUZIONE

- Un logico approccio dovrebbe prevedere la seguente sequenza di fasi:
  - investigare sull'organizzazione
  - investigare sul SG
  - investigare sulla conformità
  - investigare sull'efficacia del SG

LA CONDUZIONE

- L'efficacia del SG è più difficile da provare, ma dovrebbe essere definita giudicando il risultato dell'implementazione.
- Perciò, in ogni reparto visitato, il valutatore dovrà determinare:
  - l'esistenza del SG
  - la corretta operatività del SG
  - l'efficacia del SG

LA CONDUZIONE

- Osservazioni su come procede il lavoro
  - Ci sono 4 obiettivi da perseguire mediante queste osservazioni:
    - prove di una corretta implementazione di procedure e pratiche
    - prove di una comprensione delle procedure e del SG
    - prove di adeguatezza delle risorse umane e materiali
    - prove dell'efficacia del sistema per ottenere qualità

LA CONDUZIONE

- Valutazione delle attrezzature, risorse, impianti
  - Scopo di questa valutazione è la verifica che l'azienda possieda mezzi, risorse umane e materiali a sostegno adeguato della qualità.
- Discussioni o interviste con il personale
  - Permettono di definire la comprensione, la conoscenza di ruoli e la responsabilità del personale.

LA CONDUZIONE

- Dichiarazione dei rilievi
  - L'obiettivo dell'Audit del SG è stabilire la conformità e verificare che il SG sia correttamente applicato.
  - Le richieste violate/disattese possono riguardare:
    - quanto è richiesto da specifiche e da norme di QA
    - quello che i manuali, le procedure, le documentazioni di lavoro e le istruzioni operative affermano debba essere fatto
    - una richiesta di un codice, una pratica o un contratto

LA CONDUZIONE

- Una non conformità è definita come:
  - non soddisfacimento dei requisiti specificati

LA CONDUZIONE

- Il valutatore deve essere in grado di dimostrare la reale evidenza che quanto riscontrato si verifichi effettivamente.

- L'evidenza può essere:
  - qualche cosa che il valutatore ha visto
  - qualche cosa che il valutatore ha sentito da parte di un rappresentante della società come formalmente o praticamente accettata
  - qualche cosa che il valutatore ha sentito dai rappresentanti della società riguardo il loro modo di applicare il SG

LA CONDUZIONE

- Sulla base dell'evidenza di ciò il valutatore scrive una dichiarazione di rilievo, che contiene:
  - l'individuazione della prescrizione rispetto alla quale si è riscontrata la non conformità e una breve spiegazione del significato della prescrizione;
  - la reale evidenza riscontrata dal valutatore;
  - eventuali dettagli reali per consentire al management di capire e identificare dove la non conformità è avvenuta e cosa fosse.

LA CONDUZIONE

- I rilievi sono di grande importanza nella VI del SG a causa dello scopo per il quale vengono usati e cioè:
- registrare la reale evidenza sulla base della quale il RVI giunge alla valutazione conclusiva in quanto tutte le valutazioni conclusive devono essere supportate da evidenze
- informare il management sulle non conformità scoperte dalla verifica
- prevedere un punto di partenza per il piano delle azioni correttive che seguirà la valutazione

LA CONDUZIONE

- Allorché il valutatore è convinto che ci sia una non conformità deve:
  - discutere il problema con il rappresentante della società
  - dire al rappresentante della società quale sia la non conformità e quale sia stata la sua prova
  - prendere opportune note relative

LE RICHIESTE DI AZIONI CORRETTIVE

- Richieste di azioni correttive (RAC)
  - Al termine delle analisi relative alla valutazione eseguita e dell'esame dei rilievi emersi, nei casi di non conformità, è necessario emettere le RAC.

LE RICHIESTE DI AZIONI CORRETTIVE

- Registro delle RAC
  - L'organizzazione che ha condotto la valutazione dovrebbe sempre mantenere un registro delle RAC emesse.
  - Lo scopo finale è sempre il miglioramento del SG indipendentemente da obiettivi di certificazione. Le conseguenti RAC dovranno essere comunque implementate allo scopo di soddisfare l'obiettivo della VI.

LE RICHIESTE DI AZIONI CORRETTIVE

- Le RAC possono essere classificate in base alla criticità delle carenze riscontrate, in particolare:
  - NON CONFORMITA' MAGGIORI: fondamentali per il sistema; la loro presenza indica che il SG non rispetta la conformità alle norme (non conformità estese)
  - NON CONFORMITA' MINORI: sono errori minori, magari causati da un operatore che non applica il sistema, piuttosto che da difetti di impostazione del SG

RIUNIONE DI CHIUSURA

- Riunione di chiusura V.I.
- I risultati e le conclusioni del gruppo di valutazione sono presentati all'organizzazione verificata in un modulo riassuntivo durante la riunione alla quale partecipa l'intera rappresentanza della commissione di valutazione e dei delegati della commissione valutata.

RIUNIONE DI CHIUSURA

- Durante la riunione di chiusura è fondamentale:
  - comunicare con chiarezza i "pro" e i "contro"
  - assicurarsi che le NC siano accettate e condivise
  - cercare di individuare le cause dei problemi
  - cooperare nell'individuarne le soluzioni
  - lasciare spazio per chiarimenti, domande
  - sottolineare che tutte le risultanze sono riferite ad un "campione"

RIUNIONE DI CHIUSURA

- VI di prima parte
  - Nel caso di una VI interna, la riunione formale di chiusura non è necessaria e ogni discussione dovrebbe essere informale
- VI di seconda parte
  - Molto spesso è eseguita quando contratti importanti sono al punto di approvazione e il responsabile della verifica ispettiva deve essere consapevole che il rapporto dell'audit può essere usato dopo come punto di riferimento per risolvere possibili dispute.

RIUNIONE DI CHIUSURA

- VI di terza parte
  - In questo caso l'organizzazione verificata è il cliente dell'ente di certificazione. E' consuetudine che i valutatori leggano ogni riscontro e diano una spiegazione verbale alla direzione.

LA VERBALIZZAZIONE

- Dichiarazioni dell'esito
  - Il gruppo di VI deve sempre includere una dichiarazione dell'esito alla chiusura della riunione. Nel caso di valutazioni di terza parte la dichiarazione dell'esito è una richiesta formale.
  - Prima che i valutatori lascino il campo, i rappresentanti dell'organizzazione devono conoscere esattamente quali non conformità sono state individuate e quali conclusioni il gruppo ha raggiunto, per poter trasferire tali informazioni ai propri superiori.

LA VERBALIZZAZIONE

Il rapporto DOVREBBE contenere	**Il rapporto NON DOVREBBE contenere**
identificazione dell'organizzazione verificata	deficienze riscontrate e risolte durante la verifica
data e luogo della valutazione	informazioni confidenziali ottenute durante la verifica
obiettivi della valutazione, norme di riferimento	argomenti non espressi e non discussi durante la riunione di chiusura
persone contattate durante la valutazione	opinioni soggettive
nome dei valutatori membri del gruppo	dichiarazioni ambigue
risultati della valutazione, RAC emessi	frasi contraddittorie
data della riunione di chiusura	
lista dei partecipanti	
dichiarazione finale	
lista di distribuzione	
lista di allegati	

LE AZIONI SUCCESSIVE ALLA VI

- Proposte di azioni correttive
  - Queste non possono essere discusse nella riunione finale.
  - Prima che le azioni correttive possano essere decise è necessario che siano approfondite dal personale responsabile dell'organizzazione verificata.
  - Le considerazioni su tutti gli aspetti coinvolti e la proposta di azioni correttive è opportuno che vengano proposte dal responsabile della funzione interessata.

LE AZIONI SUCCESSIVE ALLA VI

- Esecuzione delle azioni correttive richieste
  - E' importante ricordare che:
    - il responsabile dell'area dove le non conformità sono state rilevate può non essere l'esclusivo responsabile della non conformità
    - le RAC possono richiedere l'intervento di più persone
    - nel caso di VI interne il valutatore dovrebbe sempre cercare di ricavare le necessarie direttive dal management, al fine di focalizzare la VI sugli aspetti più importanti

LE AZIONI SUCCESSIVE ALLA VI

- Verifica della chiusura delle azioni correttive
  - E' necessario eseguire una successiva riverifica delle aree trovate non conformi.
  - Il processo di ricevere le proposte di azioni correttive e sorvegliarle mediante un registro completo è chiamato sorveglianza o follow-up.
  - La registrazione finale dell'implementazione e il riconoscimento della stessa è chiamato chiusura.

LE AZIONI SUCCESSIVE ALLA VI

- Sorveglianza
  - A supplemento della VI possono essere organizzate visite di sorveglianza, per assicurare il soddisfacimento dei requisiti fissati per la qualità.
  - La sorveglianza ha lo scopo ristretto di investigare solo gli specifici aspetti del sistema relativi al contratto in corso.
  - Nel caso di valutazioni di terza parte gli organismi di certificazione conducono una prima valutazione completa rispetto alle specifiche e altre, successivamente, a periodi stabiliti.

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo V

Ing. Salvatore Minucci

ARGOMENTO 5

CASI PRATICI DI UN'ATTIVITÀ DI AUDIT

TEST 01

- testo -

Il dott. Verifico ha ricevuto l'incarico di condurre una verifica ispettiva presso l'azienda "Subisco & Soffro", volta a valutare la conformità del suo sistema di gestione per la protezione dei dati personali ai requisiti del GDPR.

La "Subisco & Soffro" produce e commercializza capi d'abbigliamento, che distribuisce attraverso una propria rete di logistica, e che in parte vende in un suo punto vendita.

Il dott. Verifico non ha alcuna ulteriore informazione sull'azienda; dalla visione del sito internet dell'azienda rileva che la stessa svolge anche attività di e-commerce.

Prima di pianificare il programma ed il piano degli audit, il dott. Verifico procede alla conduzione di una prima verifica documentale del sistema. A tal fine predispone un elenco di richieste di documenti da sottoporre all'azienda.

Si predisponga un elenco della documentazione che il dott. Verifico dovrebbe richiede all'azienda.

TEST 01

- esempio di soluzione -

N.	**Documento Richiesto (se disponibile)**
1)	***Organigramma con ruoli privacy***
2)	***Funzionigramma***
3)	***Procedure adottate per garantire la protezione dei dati:*** Esempio: o Procedure HR: es. assunzione, dismissione e formazione dipendente o collaboratore, - Regolamento strumenti in dotazione (es. email, pc, web) o Procedure Marketing, profilazione, geo-localizzazione o Procedure IT (es. Disaster recovery, cyber risk, back up, Impact assessment, Risk Assessment, Privacy by design e by default, etc) o Procedura di data cancellation, destruction e retention o Procedura biometria (es. firma grafometrica) e rilevamento immagini e impronte digitali o Procedura Data Breach Notification o Recupero crediti o Fatturazione o Finalità difensive o Cloud provider o Dati aggregati anonimi e non anonimi o Trasferimenti dati estero o Procedure per raccolta di consensi e fornitura informativa o Procedure per l'esercizio dei diritti dell'interessato o Codici di condotta o Certificazioni GDPR o Procedura per registrazione conversazioni telefoniche o Procedure di comunicazioni all'interessato e al Garante in caso di accessi non autorizzati ai dati del cliente
4)	***Informativa privacy ai dipendenti e/o collaboratori (Template)***
5)	***Informativa privacy ai candidati (Template)***
6)	***Informativa privacy ai visitatori (Template)***
7)	***Informativa privacy ai fornitori (Template)***
8)	***Informativa privacy ai clienti (Template)***

9)	***Informativa privacy ai clienti potenziali (Template)***
10)	***Informativa privacy agli utenti registrati o non registrati per tutti i siti web (Template)***
11)	***Informativa privacy agli utenti di carte fedeltà o di abbonamenti premi fedeltà (Template)***
12)	***Informativa privacy ai partecipanti di concorsi a premio (Template)***
13)	***Informativa App (Template)***
14)	***Informativa Videosorveglianza (Template)***
15)	***Informativa Geo-localizzazione (Template)***
16)	***Informativa Biometria (es. per uso di firma biometrica e grafometrica)***
17)	***Accordo con le rappresentanze sindacali o autorizzazione della DTL relativi alla Videosorveglianza***
18)	***Lista Cookie siti web*** Elenco di tutti i cookies utilizzati sul sito e relative finalità: es. cookie tecnici, analitici, profilazione. Elenco eventuali tecnologie fingerprinting usate.
19)	***Cookie (e fingerprinting) Policy di siti web***
20)	***Banner Cookie (e fingerprinting) di siti web***
21)	***Form di consenso cittadini, fornitori, utenti web al trattamento dei dati (ad esempio al trattamento di dati sensibili, al trattamento per finalità di marketing, geolocalizzazione, profilazione, biometrica etc.) (Template)***
22)	***Form di consenso cittadini, fornitori, utenti web alla comunicazione dei dati a terzi (ad esempio per finalità di marketing o profilazione) (Template)***
23)	***Form di consenso cittadini, fornitori, utenti web all'uso delle immagini (Template)***

24)	***Form di consenso dipendenti, cittadini, fornitori, utenti web al trattamento al trasferimento dati extra EU (Template)***
25)	***Nomina incaricati al trattamento (Template)***
26)	***Nomina incaricati della videosorveglianza (Template)***
27)	***Nomina incaricati della custodia delle chiavi (psw/chiavi fisiche) (Template)***
28)	***Nomina responsabili interni del trattamento (Template)***
29)	***Nomina responsabili esterni del trattamento (Es. Provider IT, Template)***
30)	***Nomina degli amministratori di sistema (Template)***
31)	***Nomina dell'Ente come responsabile esterno del trattamento di terzi soggetti (titolari autonomi es. clienti o banche etc) (Template)***
32)	***Contratti con dipendenti e collaboratori con eventuali clausole privacy (Template)***
33)	***Contratti con clienti e fornitori con eventuali clausole privacy (Template)***
34)	***Nomina Privacy Officer (DPO)***
35)	***Lista aggiornata degli incaricati al trattamento***
36)	***Lista aggiornata dei responsabili del trattamento interni***
37)	***Lista aggiornata dei responsabili esterni (compresi fornitori che trattano dati per conto dell'Ente)***

38)	***Lista aggiornata degli amministratori di sistema della Ente***
39)	***Lista dei database utilizzati***
40)	***Lista siti web***
41)	***Lista delle misure e procedure di sicurezza adottate, elettroniche e non elettroniche, previste dalla legge***
42)	***Registri dei trattamenti con dettaglio di tutti i trattamenti posti in essere sulla base del Regolamento Privacy***
43)	***Formazione periodica incaricati e registro aggiornato della formazione***
44)	***Lista Contenziosi privacy***
45)	***Lista comunicazioni all'interessato e al Garante in caso di accessi non autorizzati ai dati del cliente***
46)	***Report claims privacy***
47)	***Report esercizio diritti interessato***
48)	***Eventuali altri documenti/policy/procedure rilevanti ai fini della protezione dei dati personali***

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo V

Ing. Salvatore Minucci

ARGOMENTO 5

CASI PRATICI DI UN'ATTIVITÀ DI AUDIT

TEST 02

- testo -

Il dott. Verifico, in preparazione di un Audit presso l'azienda "Subisco & Soffro", ha ricevuto da parte della stessa un documento denominato "Modello di consenso informato per i lavoratori dipendenti". Tale documento costituisce l'informativa fornita ai dipendenti, in fase di assunzione, in relazione alla gestione dei loro dati personali.

Il dott. Verifico ci sottopone documento chiedendoci di individuare eventuali non conformità rispetto ai requisiti del GDPR e di segnalare osservazioni e commenti da utilizzare in preparazione dell'Audit presso l'Azienda.

Si esamini il documento ricevuto, e si rediga la nota da inviare al dott. Verifico.

TEST 02

- documento da esaminare -

LOGO AZIENDALE

Egregio Signor
Nome Cognome

Oggetto : MODELLO DI CONSENSO INFORMATO PER I LAVORATORI DIPENDENTI

La scrivente Società comunica che, per l'instaurazione e la gestione del rapporto di lavoro con Lei in corso, è titolare di dati Suoi e dei Suoi familiari (1) qualificati come dati personali ai sensi d.lgs. 196/03 e del Regolamento UE 2016/679 (GDPR).

1) La informiamo, pertanto, che tali dati verranno trattati con il supporto di mezzi cartacei, informatici o telematici:
   - per l'eventuale assunzione, laddove questa non sia già intervenuta;
   - per l'elaborazione ed il pagamento della retribuzione;
   - per l'adempimento di tutti gli obblighi legali e contrattuali, anche collettivi, connessi al rapporto di lavoro;
2) Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità per l'azienda di dare esecuzione al contratto o di svolgere correttamente tutti gli adempimenti, quali quelli di natura retributiva, contributiva, fiscale ed assicurativa, connessi al rapporto di lavoro;
3) Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati in Italia e trasferiti all'estero esclusivamente per le finalità sopra specificate a:
   - Enti pubblici (INPS,INAIL,Direzione prov. del lavoro, Uffici fiscali);
   - Professionisti o Società di servizi per l'amministrazione e gestione aziendale che operino per conto della nostra azienda;
   - Fondi o casse anche private di previdenza e assistenza;
   - Studi medici in adempimento degli obblighi in materia di igiene e sicurezza del lavoro;
   - Società di assicurazioni e Istituti di credito;
   - Organizzazioni sindacali cui lei abbia conferito mandato;
4) In relazione al rapporto di lavoro, l'azienda potrà trattare dati che la legge definisce "sensibili" o “particolari” in quanto idonei a rilevare ad esempio:
   a) uno stato generale di salute (assenze per malattia, maternità, infortunio o l'avviamento obbligatorio) idoneità o meno a determinate mansioni (quale esito espresso da personale medico a seguito di visite mediche preventive periodiche o richieste da Lei stesso/a);
   b) l'adesione ad un sindacato (assunzione di cariche e/o richiesta di trattenute per quote di associazione sindacale), l'adesione ad un partito politico o la titolarità di cariche pubbliche elettive (permessi o di aspettativa),convinzioni religiose(festività religiose fruibili per legge);
5) Tutti i dati predetti e gli altri costituenti il Suo stato di servizio verranno conservati anche dopo la cessazione del rapporto di lavoro per l'espletamento di tutti gli eventuali adempimenti connessi o derivanti dalla conclusione del rapporto di lavoro stesso.
6) Titolare del trattamento dei Suoi dati personali è
   Nome azienda - Con sede in **sede**, nella figura del suo Amministratore sig. **Nome Amministratore**
7) Relativamente a dati personali in nostro possesso l'interessato può esercitare i diritti previsti dall'art. 7 del d. lgs. 196/03, che si allega in copia e degli art. da 15 a 21 del Regolamento UE 2016/679 (GDPR), che si allegano.

NOME AZIENDA
L'Amministratore
Nome Amministratore

Il /i sottoscritto/i (1) in calce identificato/i dichiara/no di aver ricevuto completa informativa ai sensi degli artt. 11 e 13 del d. lgs. 196/03, unitamente a copia dell'art. 7 del medesimo provvedimento legislativo, e degli articoli da 15 a 21 del Regolamento UE 2016/679 (GDPR), unitamente ad una copia degli stessi, ed esprime/o no il consenso al trattamento ed alla comunicazione dei propri dati qualificati come personali dalla citata legge con particolare riguardo a quelli cosiddetti sensibili nei limiti, per le finalità e per la durata precisati nell'informativa.

FIRMA

.....

(1)

COGNOME NOME	REL. DI PARENTELA	FIRMA
.....	.....	.....
.....	.....	.....
.....	.....	.....

(1) Quando si trattino anche dati relativi ai familiari (ad esempio assegni per il nucleo familiare, permessi per assistenza ai familiari, ecc.). Il consenso deve essere sottoscritto dai familiari maggiorenni.

ART. 7 del d. lgs. 196/03 - Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente
   sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

ART. 26. - Garanzie per i dati sensibili

1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.

Regolamento UE 2016/679 (GDPR)

Articolo 15

Diritto di accesso dell'interessato

1. L'interessato ha il 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 seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) 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.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

Articolo 16

Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 17

Diritto alla cancellazione («diritto all'oblio»)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Articolo 18

Diritto di limitazione di trattamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) 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.

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Articolo 19

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Articolo 20

Diritto alla portabilità dei dati

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Articolo 21

Diritto di opposizione

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

TEST 02

- esempio di soluzione -

Nota per il dott. Verifico:

L'informativa ai dipendenti appare sostanzialmente adeguata.

In fase di verifica in campo, verificare quali soggetti accedano effettivamente ai dati personali dei dipendenti, la loro qualifica, l'eventuale trasferimento extra UE (non menzionata nel documento), le modalità reali di esercizio dei diritti degli interessati.

Verificare anche in che modo l'Azienda abbia provveduto ad informare i dipendenti già in forza alla data di inizio utilizzo del form esaminato, e che quindi potrebbero non aver ricevuto adeguata informativa.

Corso di Formazione Manageriale

Responsabile protezione dei dati "DPO" UE 2016/679

Modulo V

Ing. Salvatore Minucci

ARGOMENTO 5

CASI PRATICI DI UN'ATTIVITÀ DI AUDIT

TEST 03

- testo -

Il dott. Verifico, in preparazione di un Audit presso l'azienda "Subisco & Soffro", ha ricevuto da parte della stessa un documento denominato "<u>Lettera di Incarico</u>". Tale documento costituisce la "<u>Nomina ad incaricato del trattamento</u>".

Il dott. Verifico ci sottopone documento chiedendoci di individuare eventuali non conformità rispetto ai requisiti del GDPR e di segnalare osservazioni e commenti da utilizzare in preparazione dell'Audit presso l'Azienda.

Si esamini il documento ricevuto, e si rediga la nota da inviare al dott. Verifico.

TEST 03

- documento da esaminare -

LOGO AZIENDALE. **LETTERA DI INCARICO**

Il sottoscritto Xxxxxx Xxxxx, in qualità di Amministratore della **"Subisco & Soffro".** che ai sensi del Regolamento UE 2016/679 del 27 Aprile 2016 si configura quale "Titolare del Trattamento" di dati personali, ed in virtù del rapporto di lavoro in essere con il sig. **Yyyyy Yyyyyy** e delle mansioni e dei compiti ad egli assegnati, con la presente gli affida l'incarico di **INCARICATO DEL TRATTAMENTO**.
Quale Incaricato del Trattamento, il sig. Yyyyyy Yyyyyy ha tra i suoi compiti quelli di:

- Svolgere una o più operazioni, con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali. Rientrano tra le operazioni sui dati personali: 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.

Con il termine "dato", si intende qualsiasi "dato personale" come definito nel Regolamento UE 2016/679 e come appresso riportato: "qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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".
Esempi di "dati personali" sono quindi i dati personali relativi ai dipendenti, ai fornitori, ai clienti, ai consulenti esterni.

Disposizioni generali:

- L'incaricato del trattamento è autorizzato ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito degli incarichi assegnati, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.
- Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste nell'ambito delle mansioni e dei compiti ad egli assegnati, l'incaricato si impegna quindi ad accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti ad egli assegnati.
- L'incaricato del trattamento è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità previste nell'ambito delle mansioni e dei compiti ad egli assegnati.
- In particolare, qualora i dati siano trattati utilizzando sistemi informatici, l'incaricato deve conservare con la massima segretezza le credenziali di autenticazione ed eventuali dispositivi di autenticazione in suo possesso e uso esclusivo.
- L'incaricato del trattamento non deve in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali, ne lasciare incustoditi o accessibili a terzi i dati trattati custoditi in forma cartacea.
- Durante l'orario di lavoro, i dati trattati in forma cartacea non devono essere mai lasciati incustoditi ed al termine dell'orario di lavoro i documenti devono essere archiviati e conservati in modo da prevenirne l'accesso non autorizzato.

- Per evitare il rischio di diffusione dei dati personali trattati, si deve evitare l'utilizzo di copie dei dati (es. copie su unità di memoria portatili, copie fotostatiche, ecc.)
- Quando i dati, nella forma di documenti o unità di memoria portatili, devono essere portati all'esterno del luogo di lavoro, l'incaricato deve tenere sempre con questi documenti o queste unità di memoria portatili.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia una persona autorizzata a potere trattare i dati in questione.
- In generale, l'incaricato adotterà ogni cautela affinché nessuna persona non autorizzata, possa venire a conoscenza o in possesso dei dati personali trattati.

Le attività di trattamento dei dati connesse ai compiti assegnati, verranno svolte presso gli uffici dell'Azienda in Vvvvvvv . Comune (PV).

Luogo e Data, _____

Il Titolare del Trattamento	L'incaricato
Xxxxxx Xxxxxxx	Yyyyyyy Yyyyyyy

TEST 03

- esempio di soluzione -

Nota per il dott. Verifico:

L'informativa ai dipendenti appare redatta in modo generico ed incompleto.

In particolare non sono specificati i dati personali di cui si autorizza il trattamento, e non sono specificate le istruzioni all'incaricato in materia di Data Breach.

Per tanto, l'informativa non costituisce un'adeguata delega di funzioni.

In fase di verifica in campo, confermare le risultanze di questa analisi ed eventualmente emettere una Non Conformità