Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

DOCUMENTO

IL RUOLO DEL COMMERCIALISTA IN MATERIA DI PRIVACY E PROTEZIONE DEI DATI (REG. UE 2016/679): LA VALUTAZIONE DELLA CONFORMITÀ AL GDPR

AREA DI DELEGA CNDCEC

Compliance e modelli organizzativi delle imprese

COMMISSIONE DI STUDIO

Privacy - Iscritti

CONSIGLIERA DELEGATA

Eliana Quintili

PRESIDENTE

Florianna Golino

GIUGNO 2025

Composizione del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

Presidente

Elbano de Nuccio

Vice Presidente

Antonio Repaci

Consigliere Segretario

Giovanna Greco

Consigliere Tesoriere

Salvatore Regalbuto

Consiglieri

Gianluca Ancarani
Marina Andreatta
Cristina Bertinelli
Aldo Campo
Rosa D'Angiolella
Michele de Tavonatti
Fabrizio Escheri
Gian Luca Galletti
Cristina Marrone
Maurizio Masini
Pasquale Mazza
David Moro
Eliana Quintili
Pierpaolo Sanna
Liliana Smargiassi
Gabriella Viggiano
Giuseppe Venneri

Collegio dei revisori

Presidente

Rosanna Marotta

Componenti

Maura Rosano
Sergio Ceccotti

Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

Area di delega CNDCEC "Compliance e modelli organizzativi delle imprese"

A cura della Commissione di studio "Privacy - Iscritti"

Consigliera CNDCEC delegata

Eliana Quintili

Presidente

Florianna Golino

Segretario

Paola Ianni

Componenti

Chiara Battaglia
Michele Di Cicco
Monica Donati
Valter Franco
Francesco Giuseppe Gori
Massimo Grazini
Francesco Paolo La Franca
Ezio Longhi
Giuseppe Palmiotto
Nicola Paoletti
Luigina Paturzi

Staff tecnico CNDCEC

Annalisa De Vivo

Sommario

Introduzione

L'evoluzione normativa in materia di protezione dei dati personali, culminata con l'entrata in vigore del Regolamento (UE) 2016/679 (GDPR) e con l'adeguamento del quadro nazionale attraverso il d.lgs. 196/2003, così come modificato, ha determinato una profonda trasformazione nei processi organizzativi delle imprese e delle pubbliche amministrazioni, generando nuove esigenze in termini di competenze e responsabilità. In questo scenario, la figura del Commercialista si è dimostrata particolarmente versatile e strategica, capace di affiancare con competenza e rigore le organizzazioni in un percorso di adeguamento normativo che non può prescindere da una solida impostazione metodologica.

La tutela dei dati personali, infatti, non è più solo un obbligo giuridico, ma un ambito trasversale che richiede l'integrazione di conoscenze giuridiche, informatiche, organizzative e gestionali. Il Commercialista, già fortemente radicato nel tessuto economico e imprenditoriale, si configura sempre più spesso come figura chiave in questo contesto, chiamato a svolgere non solo funzioni consulenziali, ma anche ruoli operativi di responsabilità come *data protection officer* (DPO), responsabile *audit* o esperto tecnico in contenziosi in materia di privacy.

Con il presente Documento il Consiglio Nazionale intende offrire un contributo concreto alla qualificazione dell'attività del Commercialista nell'ambito della protezione dei dati, ponendo l'accento in particolare sulla dimensione dell'*audit*, strumento essenziale per valutare il livello di conformità delle organizzazioni e garantire, attraverso evidenze documentali e procedurali, il principio di accountability. A tal fine, vengono esposte le tecniche di *audit* previste dalla norma UNI EN ISO 19011:2018, arricchite da esempi pratici di modulistica e suggerimenti operativi per la verifica della documentazione richiesta.

Particolare attenzione è dedicata anche ai sistemi di gestione volontari, come quelli basati sulle norme ISO/IEC 27001 e 27701 o sullo schema ISDP©10003:2020, strumenti sempre più adottati dalle organizzazioni come riferimento per strutturare le proprie politiche di sicurezza e compliance in materia di protezione dei dati.

Il Consiglio Nazionale ritiene fondamentale accompagnare gli Iscritti in questo percorso di crescita professionale, promuovendo l'acquisizione di competenze tecniche e metodologiche che siano al tempo stesso riconosciute a livello internazionale e concretamente spendibili nella pratica professionale. L'obiettivo non è solo quello di rafforzare il ruolo del Commercialista nella governance dei processi aziendali, ma anche di affermarne il valore aggiunto come garante della legalità, dell'etica e della trasparenza nelle relazioni economiche e istituzionali.

Eliana Quintili

Consigliera CNDCEC delegata Area "Compliance e modelli organizzativi delle imprese"

Premessa

Con l'entrata in vigore del Regolamento (UE) 2016/679 (*General Data Protection Regulation*, nel prosieguo: GDPR*)*, si è rafforzata e consolidata la necessità per le imprese e per gli Enti di avvalersi di consulenti specializzati in materia di protezione dei dati e privacy, figure necessarie per affiancare le organizzazioni, pubbliche e private, nel difficile percorso di adeguamento alle numerose previsioni contenute nella normativa vigente. Trattandosi di una materia che richiede competenze multidisciplinari, *in primis* giuridiche e informatiche, i professionisti del settore appartengono a svariate categorie professionali, si tratta, infatti, di avvocati, ingegneri, informatici e, chiaramente, di Commercialisti. Questi ultimi, in particolare, nell'ultimo periodo hanno maturato sempre più esperienza nel settore, assumendo incarichi non solo come consulenti, ma anche come Responsabili della protezione dei dati o *Data Protection Officer* (DPO) o, ancora, come *auditor*, incaricati da imprese committenti di condurre *audit* di parte seconda sui fornitori, al fine di valutarne il grado di conformità alla normativa cogente e/o ai requisiti contrattuali.

Conseguentemente, al Commercialista esperto di protezione dei dati e privacy sono richieste competenze specifiche sulla conduzione degli *audit*, sotto il profilo generale e con particolare riferimento alla *data protection*.

Obiettivo del presente lavoro è, pertanto, quello di fornire indicazioni sulle tecniche di *auditing* riconosciute da standard internazionali, largamente diffuse e utilizzate nell'ambito dei sistemi di gestione, sia dalle organizzazioni per condurre gli *audit* interni (di prima parte), sia dagli organismi di certificazione per le verifiche ispettive di parte terza, finalizzate al rilascio delle certificazioni, sia, come già accennato, per gli *audit* di parte seconda, presso i fornitori, allo scopo di fornire ai Commercialisti un utile strumento metodologico (oltre che universalmente riconosciuto), da utilizzare nell'espletamento dei propri incarichi in materia di privacy.

Il documento, quindi, riporta sinteticamente le tecniche di conduzione degli *audit* di cui alla norma UNI EN ISO 19011:2018, fornendo esempi di modulistica da utilizzare durante le verifiche e, inoltre, si sofferma sulla documentazione da richiedere alle organizzazioni ai fini dell'*accountability*. Nella trattazione delle misure organizzative e tecniche da sottoporre ad *audit*, adottate dalle organizzazioni a valle dell'analisi dei rischi effettuata, anche al fine di non incorrere in violazioni della normativa riconducibili a perdita, smarrimento, danneggiamento, furto e diffusione non autorizzata dei dati trattati, è doveroso il richiamo alle norme tecniche volontarie ISO/IEC 27001 e ISO/IEC 27701, standard certificabili sulla protezione dei dati che contengono anche utili indicazioni in materia di sicurezza informatica, nonché alla norma ISDP©10003:2020, schema internazionale di certificazione progettato per valutare la conformità al GDPR, conformemente alla norma UNI EN ISO 17065. Tali sistemi di gestione volontari di protezione dei dati, a prescindere dall'ottenimento della certificazione da parte degli Enti preposti, costituiscono sicuramente un ausilio per istituire e implementare correttamente procedure gestionali orientate alla conformità normativa e all'*accountability*, principio su cui si fonda l'intero impianto normativo costruito dal legislatore europeo.

Capitolo primo

GLI *AUDIT* SULLA CONFORMITÀ AL GDPR

1.1. Definizione di *audit* e tipologie: la norma UNI EN ISO 19011:2018

Nel paragrafo 3.1 dell'ultima versione della norma tecnica UNI EN ISO 19011, l'*audit* viene definito come "*Processo sistematico, indipendente e documentato per ottenere evidenze oggettive e valutarle in modo obiettivo, al fine di stabilire in quale misura sono soddisfatti i criteri dell'audit*", ovvero, come specificato al par. 3.7, l'*audit* si configura come un'attività che mira a verificare se siano soddisfatti i requisiti di riferimento, che, in base alla specifica finalità dell'*audit* condotto, possono derivare da leggi, regolamenti, politiche, norme o prassi di settore, procedure interne, e rispetto ai quali vengono confrontate le evidenze oggettive, raccolte durante l'attività in campo. Vengono commissionati e condotti *audit* per una grande varietà di scopi e, indipendentemente da quali essi siano, lo standard fornisce una guida per la loro conduzione, oltre che per il corretto comportamento da tenere per gli *auditor*. La norma si focalizza su *audit* di prima parte (interni) e di seconda parte (su fornitori o altre parti interessate), ma specifica chiaramente che può essere utilizzata come riferimento anche in *audit* esterni di parte terza (per fini legali, regolamentari o condotti da organismi accreditati per il rilascio delle certificazioni), ai quali propriamente si applica, per i percorsi di certificazione, la norma ISO/IEC 17021.

La norma è adatta per tutte le organizzazioni, indipendentemente dalle dimensioni o dal settore, che debbano pianificare ed eseguire *audit* (su qualsiasi materia) e risulta un utile riferimento anche per i professionisti che intendano condurre un *audit* indipendente, a qualsiasi scopo.

Tralasciando i primi due capitoli, relativi all'introduzione, allo scopo e al campo di applicazione, nella tabella seguente si riporta la struttura della norma, con i contenuti:

Capitolo	Contenuto
3	Termini e definizioni
4	Principi dell'attività di *audit*
5	Gestione di un programma di *audit*
6	Conduzione di un *audit*
7	Competenza e valutazione degli *auditor*
Appendice A	Contributi pratici per la pianificazione e conduzione dell'*audit*

Tra i termini e le definizioni, oltre a quelle già richiamate di audit e di criteri dell'*audit*, è utile sottolineare quella di "risultanze dell'audit" (par. 3.10), come "*esito della valutazione delle evidenze*

dell'audit raccolte" sempre rispetto ai criteri dell' audit che ci si sia prefissati, risultanze che possono indicare conformità o non conformità rispetto ai criteri di *audit*, «compliance» o «non compliance» rispetto a requisiti di legge o regolamentati e mettere in evidenza scenari di rischio, opportunità di miglioramento, valide prassi operative. Le "conclusioni dell'audit" (par. 3.11) ne costituiscono gli esiti, a valle dell'attività svolta e delle risultanze ottenute.

Il capitolo quarto riporta i **Principi dell'attività di audit** che, se rispettati, rendono l'attività di audit efficace e affidabile, consentendo all'organizzazione sottoposta ad *audit* di prendere decisioni nell'interesse dell'organizzazione in relazione agli esiti e agli auditor di pervenire, a parità di situazioni, a conclusioni simili.

I principi da rispettare sono riassumibili in:

- integrità;
- presentazione imparziale;
- dovuta professionalità;
- riservatezza;
- indipendenza;
- approccio basato sull'evidenza;
- approccio basato sul rischio.

L'*auditor* dovrà, cioè, riportare gli esiti in modo accurato e veritiero, applicare diligenza e giudizio nell'esecuzione dell'audit, essere indipendente per garantire l'imparzialità dell'audit e l'obiettività delle conclusioni, mantenere la riservatezza su tutte le informazioni raccolte durante l'attività ispettiva per garantire la sicurezza dei dati, dovrà avere un approccio che consideri rischi e opportunità per l'organizzazione e basarsi sulle evidenze raccolte, per giungere a conclusioni affidabili e riproducibili.

1.2. La pianificazione e la gestione degli *audit*

Fatte queste premesse, la norma si sofferma sull'iter procedurale da seguire prima, durante e dopo la conduzione degli *audit*, partendo dall'importante fase della pianificazione e delineando un flusso di processo per la **Gestione del programma di *audit***. Andranno quindi preliminarmente definiti gli obiettivi del programma di audit, valutando rischi e opportunità (*risk based thinking*), definito il programma, avviata e preparata l'attività, per poi attuare il programma e condurre l'audit. Al termine della verifica si preparerà e distribuirà agli interessati il rapporto di *audit*. Monitorato il rispetto del programma, si chiude l'attività, riesaminando il programma ai fini del miglioramento e si conducono le eventuali azioni successive di *follow up.*

L'attuazione (o **Conduzione**) deve avvenire secondo le fasi di seguito riportate:

1. Avvio

2. Preparazione
3. Esecuzione
4. Preparazione e distribuzione del rapporto
5. Chiusura
6. *Follow-up* (azioni successive) dettagliatamente analizzate nello standard

Particolare attenzione va rivolta alla fase di preparazione dell'*audit*, relativamente ai criteri di campionamento e raccolta delle informazioni documentate e alle liste di controllo da utilizzare. Metodi principali per raccogliere informazioni (6.4.7) da inserire nelle check list di controllo sono:

- interviste;
- osservazioni (di processi e attività);
- riesame informazioni documentate.

Utili guide pratiche sono presenti nell' Appendice A della norma.

Molto importanti sono anche le riunioni di apertura (6.4.3) e di chiusura (6.4.10). La riunione di apertura dell'*audit*, in presenza della direzione o di un suo rappresentante, ha lo scopo di:

- confermare l'accordo sui termini del piano di *audit*, da parte di tutti i soggetti coinvolti;
- presentare i membri del team di *audit* con relativi ruoli e responsabilità;
- ottenere conferma sulla possibilità di attuare tutte le attività pianificate.

La riunione di chiusura, invece, al termine delle attività, condotta dal Responsabile gruppo di *audit*, con la presenza degli altri auditor e dei responsabili delle varie aree sottoposte ad audit, rappresenta il momento in cui vengono esposte le risultanze della verifica e vengono tratte le conclusioni finali.

Le risultanze dell'*audit* (6.4.8) emergono dal confronto tra le evidenze raccolte e i criteri definiti dell'audit.

Esse possono dare origine a:

- conformità;
- non conformità;
- raccomandazioni;
- opportunità di miglioramento;
- buone prassi applicate;
- tendenze positive o negative.

Nel caso in cui emergano delle "non conformità", ovvero il mancato soddisfacimento di requisiti obbligatori, saranno richieste all'organizzazione, a seconda dei casi, azioni di "trattamento" delle non conformità, che eliminano l'anomalia rilevata, oppure anche "azioni correttive", al fine di eliminare le cause della non conformità occorsa per evitarne la ripetibilità. Tali azioni dovranno essere attuate e

documentate nei termini prefissati dall'auditor (nel caso dei processi di certificazione questi sono previsti dal Regolamento dell'Organismo di Certificazione prescelto).

Le conclusioni (6.4.9) possono riguardare:

- la conformità ai criteri di riferimento del sistema sottoposto ad *audit*;
- l'efficacia del sistema per il raggiungimento degli obiettivi e la sua capacità di gestire rischi e di attuare azioni adeguate;
- l'efficace attuazione, mantenimento e miglioramento del sistema e dei processi;
- l'efficacia del processo di riesame e le tendenze del sistema;
- la messa in evidenza di risultanze similari su diverse aree o ripetitive rispetto ad audit precedenti.

L'*audit* si considera chiuso (6.6) quando tutte le attività previste sono state effettuate ed è stato emesso il "Rapporto di *audit*" (6.5.1), ovvero un rapporto finale, redatto dal Responsabile del team di *audit*, che riporti le conclusioni dell'audit in modo:

- sintetico, nella giusta misura;
- completo e accurato;
- chiaro e comprensibile.

Punto essenziale per la buona riuscita delle attività di auditing è sicuramente la **competenza degli *auditor*,** cui la norma dedica un intero capitolo (il capitolo 7), in quanto determinante ai fini dell'affidabilità del processo e dei risultati. Gli auditor dovrebbero avere le conoscenze e abilità necessarie di carattere generale e di carattere specifico della disciplina e settore oggetto di audit e inoltre adottare comportamenti adeguati durante la conduzione dell'audit, dettagliatamente descritti al punto 7.2 della norma e di seguito riportati:

- rispettosi dei principi etici;
- di mentalità aperta, collaborativi;
- diplomatici nei rapporti interpersonali;
- dotati di spirito d'osservazione;
- perspicaci;
- versatili, predisposti al miglioramento;
- tenaci, in grado di agire con fermezza;
- risoluti e sicuri di sé, autonomi;
- sensibili alle diversità culturali.

1.3. La modulistica dedicata

Tutto quanto previsto dalla norma 19011 ed esposto al paragrafo precedente, che si sostanzia in un procedimento rigoroso di conduzione di qualsivoglia verifica ispettiva, può essere pienamente applicato agli audit finalizzati alla verifica di conformità al GDPR, presso qualsiasi organizzazione. Si riportano di seguito esempi di modulistica utilizzabile in fase di pianificazione e conduzione di tale tipologia di audit, in particolare i modelli di:

1. PIANO DI *AUDIT*;
2. LISTA DI RISCONTRO;
3. REPORT DI *AUDIT*.

PIANO DELL'AUDIT			**Rev .. del ……. Pag. 4 di 16**
Organizzazione:	Data audit:	Ora di inizio:	Sede:
Auditor	Nome e Cognome:	Ruolo:	
Obiettivo dell'*audit*			
Campo di applicazione			

Orario	Ambito	Funzioni coinvolte
	Riunione di apertura	Direzione – DPO –Amministratore di sistema
	Organigramma, nomine, ambiti di trattamento, istruzioni operative, formazione soggetti autorizzati al trattamento. Analisi dei rischi - DPIA e misure organizzative di mitigazione dei rischi	Direzione o un suo rappresentante
	Informative agli interessati	Direzione o un suo rappresentante - Amministratore di sistema
	Procedure *data breach*	Direzione - Amministratore di sistema
	Policy aziendali	Direzione - Amministratore di sistema
	Misure tecniche di mitigazione dei Rischi	Amministratore di sistema
	Riunione di chiusura	Direzione – DPO -Amministratore di sistema

DATA _____ FIRMA

_____

LISTA DI RISCONTRO	Rev … del ….. Pag. 5 di 16

Processo/Funzione sottoposti ad *audit*:

ELEMENTO DI CONTROLLO	Rif. normativo	EVIDENZA OGGETTIVA	ESITO

LEGENDA: **C** = conforme **NC** = non conforme **OSS** = osservazione

NOTE:

Data: Firma Auditor

RAPPORTO DI AUDIT	Rev …. del …… Pag. 6 di 16

Rapporto n° Data:

Processo / Funzione auditati:

Persone intervistate:

Argomenti esaminati:

TEAM DI VERIFICA ISPETTIVA

Responsabile: _____ Ispettori: /

Osservatori: _____ / _____ /

ESITO (*): ELEMENTI DI RISCONTRO (Vedi lista di riscontro allegata)

(*) **Positivo**; **Positivo *con riserva*** (vedere osservazioni); **Negativo** (necessità di AC)

NC/Oss	Rif. normativo	Descrizione delle Non conformità (NC) e delle Osservazioni (Oss) riscontrate

EVENTUALI PROVVEDIMENTI:

AC/AP NO SI n° _____ del _____ Firma Responsabile:

Firma Responsabile Team di Verifica: Firma Responsabile attività verificata:

Copia del presente rapporto è distribuito a:

Di seguito si riporta la **procedura del programma di audit** (PdA) in **forma sequenziale**, seguendo il ciclo **PLAN – DO – CHECK – ACT**:

PLAN – Pianificazione del programma di audit

1. Definizione degli obiettivi del programma di audit
2. Determinazione e valutazione dei rischi e delle opportunità del PdA
3. Definizione del programma di audit

DO – Attuazione del programma di audit

4. Attuazione del programma di audit
5. Avvio dell'audit
6. Preparazione delle attività di audit
7. Conduzione delle attività di audit
8. Preparazione e distribuzione del rapporto di audit

CHECK – Verifica e chiusura

9. Chiusura dell'audit
10. Monitoraggio del programma di audit

ACT – Miglioramento continuo

11. Conduzione delle azioni successive all'audit (*follow-up*)
12. Riesame e miglioramento del PdA

1.4. Le norme ISO/IEC 27001 e ISO/IEC 27701

Sulle certificazioni in ambito privacy, il GDPR chiarisce che l'adesione da parte del responsabile del trattamento ad un meccanismo di certificazione approvato, di cui all'art. 42, può essere utilizzato come strumento per aiutare il titolare o il responsabile a dimostrare il rispetto al principio di accountability.

I meccanismi di certificazione di cui all'art. 42 hanno come finalità quella di accertare la qualità dei trattamenti compiuti dal titolare o dal responsabile, i quali spesso consistono nella prestazione di servizi e sono eseguiti all'interno di processi complessi o singole attività.

La conferma di ciò è ravvisabile nel sesto paragrafo del medesimo art. 42 del GDPR: "Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'organismo di certificazione di cui all'art. 43 o, ove applicabile, all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione".

L'obiettivo delle certificazioni, secondo l'art. 42, sembra allineato con la motivazione che spinge le imprese e gli enti a implementare un Sistema di Gestione della Qualità (SGQ) conforme alle norme volontarie della serie ISO 9000.

È evidente che il GDPR preveda la possibilità di certificare i trattamenti dei dati, disciplinando le procedure di certificazione relative alle attività o insiemi di attività (processi) che coinvolgono i dati personali.

Di norma, i soggetti coinvolti nell'iter di certificazione sono:

- l'impresa/l'ente che richiede la certificazione;
- l'Organismo di Certificazione (OdC) accreditato che rilascia i certificati sulla base dei risultati di verifiche e vigila sulla corretta gestione dei certificati;
- l'ente di accreditamento che accredita gli OdC e controlla periodicamente il mantenimento dei requisiti previsti da parte di tali soggetti, tra cui l'imparzialità, competenza e adeguatezza. Il GDPR richiede che l'OdC debba essere accreditato dall'autorità di controllo competente o dall'ente nazionale di accreditamento o da entrambi;
- il consulente, che prepara l'azienda a sostenere la verifica ispettiva di parte terza, a cura dell'OdC prescelto.

Le principali certificazioni che possono essere acquisite in materia di privacy sono:

- ISO/IEC 27001
- ISO/IEC 27701

ISO/IEC 27001 - GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI / INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

È uno standard internazionale promosso congiuntamente dalla ISO (International Organization for Standardization) e dalla IEC (International Electrotechnical Commission) per la gestione della sicurezza delle informazioni. Tale standard definisce i requisiti necessari per pianificare, implementare, operare, monitorare, riesaminare, mantenere e migliorare continuamente il sistema di gestione per la sicurezza delle informazioni all'interno delle aziende.

Lo standard consente un approccio complessivo alla sicurezza delle informazioni in tutti gli ambiti interessati, dai documenti in formato digitale a quelli in formato cartaceo, dalle strumentazioni hardware (computer e reti) alle competenze del personale e si pone in un'ottica volta al miglioramento continuo dei sistemi di gestione e dei processi.

Le informazioni sono protette in funzione dei principi di **riservatezza** (assicura che le informazioni siano accessibili solo a coloro che sono autorizzati ad accedervi), **integrità** (salvaguarda l'accuratezza e la completezza delle informazioni), **disponibilità** (assicura che gli utenti autorizzati abbiano accesso alle informazioni e alle risorse associate quando richiesto) e protezione (tutela contro le frodi informatiche).

I requisiti forniti dallo standard sono i seguenti.

- Analisi dei rischi: Identificazione e valutazione dei rischi per la sicurezza delle informazioni che l'organizzazione potrebbe affrontare.
- Politiche di sicurezza: Definizione di politiche e procedure per gestire i rischi e proteggere le informazioni.
- Gestione delle risorse: Assegnazione di responsabilità specifiche per la sicurezza delle informazioni e fornire formazione e risorse adeguate al personale.
- Controllo degli accessi: Garantire che l'accesso alle informazioni sia limitato e controllato in base ai ruoli e ai privilegi assegnati.
- Sicurezza fisica e ambientale: Protezione delle risorse fisiche e degli ambienti in cui le informazioni sono elaborate, archiviate o trasmesse.
- Pianificazione per situazioni di emergenza: Preparazione per affrontare situazioni di emergenza o incidenti di sicurezza delle informazioni.
- Monitoraggio e revisione: Costante monitoraggio, valutazione e revisione del sistema di gestione per garantire la sua efficacia e migliorarlo continuamente.

Un progetto per l'implementazione della norma ISO/IEC 27001 richiede una serie di passaggi chiave, per garantire una corretta adozione e conformità agli standard di sicurezza delle informazioni. Deve senz'altro essere progettato e implementato un Sistema di gestione della sicurezza delle informazioni (SGSI).

Un Sistema di gestione della sicurezza delle informazioni (SGSI) è un insieme di regole che un'azienda deve stabilire per:

1. identificare le parti interessate e le loro aspettative nei confronti dell'azienda in termini di sicurezza delle informazioni
2. identificare quali rischi esistono per le informazioni
3. definire i controlli (protezioni) e altri metodi di mitigazione per soddisfare le aspettative identificate e gestire i rischi
4. fissare obiettivi chiari su ciò che deve essere raggiunto con la sicurezza delle informazioni
5. implementare tutti i controlli e le altre modalità di trattamento dei rischi
6. misurare continuamente se i controlli implementati funzionano come previsto
7. apportare miglioramenti continui per far funzionare meglio l'intero SGSI

Questo insieme di regole può essere redatto sotto forma di politiche, procedure e altri tipi di documenti, oppure sotto forma di processi e tecnologie consolidati che non sono documentati. La ISO 27001 individua i documenti richiesti, cioè quelli che devono essere prodotti come requisito minimo.

Di seguito si descrivono le fasi principali di un progetto finalizzato all'ottenimento della certificazione ISO 27001.

Avvio

- Comprensione dei requisiti: acquisire familiarità con la norma ISO/IEC 27001 e valutare come si applica all'organizzazione.
- Coinvolgimento della leadership: ottenere il supporto e l'impegno della dirigenza per garantire risorse e priorità per il progetto.

Analisi e pianificazione

- Valutazione dei rischi: identificare e valutare i potenziali rischi per la sicurezza delle informazioni all'interno dell'organizzazione.
- Definizione dello scopo e degli obiettivi: stabilire chiaramente gli obiettivi del progetto e definire lo scopo dell'implementazione.
- Assegnazione delle responsabilità: designare le persone coinvolte nel progetto e assegnare responsabilità specifiche.

Implementazione

- Sviluppo di politiche e procedure: creare politiche, procedure e linee guida per la gestione della sicurezza delle informazioni.
- Formazione e sensibilizzazione: fornire formazione al personale sull'importanza della sicurezza delle informazioni e sulle nuove politiche e procedure.
- Implementazione delle misure di sicurezza: attuare i controlli e le misure di sicurezza necessari per mitigare i rischi identificati.

Monitoraggio e revisione

- Audit interni: condurre audit interni per valutare l'efficacia del sistema di gestione della sicurezza delle informazioni.
- Raccolta e valutazione dei feedback: raccogliere feedback da dipendenti, stakeholder ed eventuali parti interessate per valutare l'efficacia e apportare eventuali miglioramenti.

Certificazione

- Valutazione di conformità: condurre una valutazione finale per assicurarsi che tutti i requisiti della norma siano stati soddisfatti.
- Certificazione: ottenere la certificazione da un ente di certificazione accreditato.

Miglioramento continuo

- Miglioramento continuo: implementare processi per continuare a monitorare, valutare e migliorare il sistema di gestione della sicurezza delle informazioni nel tempo.

- Revisione periodica: effettuare revisioni periodiche per garantire che il sistema rimanga rilevante ed efficace nel contesto dell'evoluzione delle minacce e delle esigenze aziendali.

Ottenere la certificazione ISO/IEC 27001 implica l'implementazione di questi requisiti e la conformità continua ad essi, dimostrando che un'organizzazione ha stabilito e mantiene un robusto sistema di gestione della sicurezza delle informazioni.

Molte organizzazioni scelgono di ottenere la certificazione ISO/IEC 27001 per dimostrare agli stakeholder, ai clienti e alle parti interessate l'attenzione dedicata alla sicurezza delle informazioni e l'impegno profuso nella protezione delle medesime.

La certificazione del sistema di gestione della sicurezza delle informazioni costituisce uno strumento di evidenza dell'impegno nella protezione proattiva delle informazioni; tuttavia, le organizzazioni possono decidere di progettare e implementare un sistema di gestione anche a prescindere dall'ottenimento di una certificazione, esclusivamente come strumento di garanzia della conformità alle previsioni normative. In entrambi i casi, il Commercialista può assumere un ruolo fondamentale nell'affiancare l'impresa nel percorso di implementazione del sistema di gestione.

ISO/IEC 27701 - Sistema di Gestione delle Informazioni sulla Privacy / Privacy Information Management System (PIMS)

La certificazione ISO 27701 per un Sistema di Gestione delle Informazioni sulla Privacy (PIMS) rappresenta l'estensione privacy della ISO 27001, relativa al Sistema di Gestione della Sicurezza delle Informazioni (ISMS). L'obiettivo principale della ISO 27701 è migliorare l'ISMS esistente, attraverso l'implementazione di controlli supplementari al fine di istituire, attuare, mantenere e migliorare continuamente un PIMS. Tale certificazione fornisce un quadro normativo entro il quale i responsabili del trattamento dei dati, inclusi i corresponsabili del trattamento dei dati personali, e i soggetti autorizzati al trattamento dei dati, compresi coloro che utilizzano subappaltatori, devono gestire e proteggere le informazioni personali identificabili (PII). L'obiettivo è ridurre il rischio connesso alla privacy di un individuo attraverso una gestione efficace e conforme dei dati personali.

Le organizzazioni che lavorano per ottenere la certificazione ISO 27701 devono già disporre della certificazione ISO 27001.

La ISO/IEC 27701 fornisce indicazioni a qualsiasi organizzazione responsabile del trattamento delle informazioni personali identificabili nell'ambito di un sistema di gestione della sicurezza delle informazioni; inoltre, fornisce un approccio basato sul rischio e aiuta a prevenire rischi specifici per la privacy.

Un sistema di gestione delle informazioni relative alla privacy (PIMS) ha diversi vantaggi:

- costruisce la fiducia nella capacità dell'organizzazione soggetto nella gestione delle informazioni personali, sia per i clienti sia per i dipendenti;
- è di supporto nel dimostrare la conformità con il GDPR;

- chiarisce i ruoli e le responsabilità all'interno dell'organizzazione;
- migliora la competenza interna e i processi per evitare infrazioni;
- fornisce trasparenza sui controlli stabiliti per la gestione della privacy;
- si integra facilmente con lo standard principale per la sicurezza delle informazioni ISO/IEC 27001.

Tale sistema di gestione, che costituisce un'evoluzione rispetto al modello conforme alla ISO/IEC 27001, difficilmente sarà adottato in assenza di finalità certificative. Tuttavia, esso può rappresentare un valido *benchmark*, in particolare per le organizzazioni di grandi dimensioni che trattano dati personali qualificati come "particolari" ai sensi del GDPR e che, pertanto, richiedono livelli di protezione più elevati.

Non vanno, inoltre trascurati gli standard:

- ISO/IEC 27002 in Italia recepito come UNI CEI EN ISO IEC 27002 Tecnologie Informatiche - Tecniche di sicurezza - Codice di pratica per la gestione della sicurezza delle informazioni (linea guida sulle contromisure da adottare conformemente all'Annex A della 27001);
- UNI CEI EN ISO/IEC 27017:2021 "Codice di condotta per i controlli di sicurezza delle informazioni basati su ISO/IEC 27002 per i servizi in cloud" e UNI CEI EN ISO/IEC 27018:2020 "Codice di condotta per la protezione delle informazioni di identificazione personale (PII) in cloud pubblici che agiscono come responsabili PII" (specificano i controlli di sicurezza da implementare quando si gestiscono servizi cloud. Questi due standard ampliano i controlli della ISO/IEC 27001 e introducono specifici controlli aggiuntivi).

In allegato si riporta un elenco delle evidenze oggettive, da verificare durante gli audit, sui requisiti richiesti dalla norma 27001 a fini certificativi, ma che possono essere utilizzati anche come riferimento per valutare la sola conformità alla normativa cogente (*Allegato 1*).

1.5. Lo Schema di certificazione Data Protection - GDPR accreditato in accordo con la norma EN ISO/IEC 17065:2012

La ISDP©10003:2020 è uno schema internazionale di certificazione progettato per valutare la conformità al GDPR per diverse tipologie di organizzazioni in tutti i settori merceologici, conformemente alla norma UNI EN ISO 17065.

Lo scopo dello schema è quello di fornire alle organizzazioni l'opportunità di dimostrare la propria responsabilità nell'attuare i requisiti previsti dal GDPR, incluso il monitoraggio delle procedure interne relative al trattamento e alla protezione dei dati personali. Ciò richiede un'attenzione particolare alla gestione adeguata dei rischi associati.

Per ottenere la certificazione ISDP©10003:2020, un'azienda deve preparare e tenere aggiornata la documentazione richiesta dal GDPR e, in particolare, un manuale Privacy che comprenda quanto di

seguito elencato:

1. elaborazione di uno schema dei trattamenti.
2. Preparazione di istruzioni scritte per il personale incaricato del trattamento.
3. Nomine e stipula dei contratti dei responsabili del trattamento.
4. Implementazione di procedure per monitorare gli amministratori di sistema.
5. Mantenimento di un registro dettagliato dei trattamenti dei dati.
6. Valutazione dei rischi e definizione di metriche di misurazione.
7. Adozione di una metodologia per la valutazione degli impatti e mantenimento di un registro delle valutazioni DPIA.
8. Presentazione di una relazione annuale da parte dell'Amministratore di sistema.
9. Presentazione di una relazione annuale, se nominato, da parte del Responsabile della Protezione dei Dati (DPO).
10. Implementazione di procedure che regolano la raccolta e il trattamento dei dati.
11. Adozione di una procedura per gestire i diritti dell'interessato.
12. Implementazione di procedure per modificare o cancellare dati.
13. Implementazione di procedure finalizzate a disciplinare l'adozione di misure di sicurezza (antivirus, backup, ripristino, gestione credenziali, gestione dei cookies, continuità operativa, recupero dai disastri, ecc.).
14. Implementazione di procedure per la gestione della privacy by design e by default.
15. Conduzione di audit interni per garantire la conformità.

Il Sistema di Gestione va progettato e implementato seguendo i principi di tutti i sistemi, ovvero il ciclo PDCA di pianificazione, implementazione, revisione e miglioramento (Plan-Do-Check-Act).

Anche questo schema, dunque, offre un valido supporto alle organizzazioni che intendano raggiungere la *compliance* in ambito protezione dei dati e privacy.

Capitolo secondo

I REGISTRI DELL'ACCOUNTABILITY

2.1. I principali registri da tenere

Ogni soggetto, pubblico o privato, è tenuto a garantire un trattamento corretto e sicuro dei dati personali dei terzi con cui interagisce, nel rispetto dei principi di liceità, correttezza e trasparenza. L'evoluzione normativa, culminata con il GDPR, impone che i dati siano trattati esclusivamente nei casi previsti dalla legge o previo consenso esplicito, adottando misure idonee a prevenire accessi non autorizzati, alterazioni o usi illeciti.

Il GDPR e i provvedimenti del Garante Privacy prescrivono obblighi articolati per tutti gli attori coinvolti nella protezione dei dati, fondati sul principio della responsabilizzazione (*accountability*); ciò comporta, tra l'altro, la documentazione delle attività svolte e la tenuta di registri al fine di dimostrare la conformità al quadro normativo.

Ogni titolare del trattamento, unitamente ai registri imposti, può istituire anche quelli discrezionali, in base alle esigenze specifiche.

Di seguito vengono esaminati i contenuti e le modalità di tenuta dei registi obbligatori per legge e di quelli più significativi che un consulente, incaricato di condurre un audit sulla conformità al GDPR, dovrebbe trovare in uso presso l'organizzazione:

- registro dei trattamenti dei dati personali;
- registro dell'Amministratore di Sistema;
- registro delle Violazioni (*Data Breach*);
- registro della Formazione;
- registro dei *Penetration Test*;
- registro dei *Disaster Ricovery*;
- registro dei Sub Responsabili del trattamento;
- registro dell'esercizio dei diritti da parte degli interessati;
- registro dei visitatori e della protezione della Privacy.

2.1.1 Il registro dei trattamenti dei dati personali

L'istituzione di questo registro è prevista dall'art. 30 del GDPR. Lo strumento di rilevazione è idoneo

a fornire un quadro aggiornato dei trattamenti in essere all'interno dell'organizzazione ed è un elemento indispensabile per effettuare l'analisi del rischio e la relativa valutazione, nonché l'individuazione delle misure di sicurezza: quindi, è propedeutico rispetto a tali attività.

La tenuta del registro dei trattamenti, sempre obbligatorio per le PA, costituisce un obbligo anche:

- per le imprese e le organizzazioni con oltre 250 dipendenti,
- quando il trattamento può generare rischi potenziali per i diritti e le libertà dell'interessato,
- quando vengono trattati dati "giudiziari", ovvero relativi a condanne penali o a reati,
- quando vengono trattati dati "particolari" (ad es. orientamenti politici, religiosi, sessuali, dati relativi allo stato di salute).

Il registro è comunque sempre consigliato per chiunque effettui trattamento di dati personali per scopi non privati, al fine di:

- mappare le informazioni principali relative al trattamento dei dati effettuato sia dai Titolari che dai Responsabili dei trattamenti (tipi di dati, finalità di trattamento, tempo di conservazione);
- dimostrare la propria conformità a quanto richiesto dalla normativa GDPR, qualora venisse richiesto dal Garante della Privacy, consentendo allo stesso di valutare la metodologia adottata per garantire la sicurezza dei trattamenti e il rispetto dei diritti degli interessati.

L'art. 30, par. 5 GDPR stabilisce che la tenuta del registro dei trattamenti non è obbligatoria per le imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento dalle stesse effettuato:

- possa rappresentare un rischio per i diritti e le libertà dell'interessato (a prescindere dal grado di rischio, quindi anche per rischi bassi),
- sia un trattamento non occasionale di dati personali di persone fisiche,
- riguardi le categorie particolari di dati di cui all'art. 9, par. 1 GDPR, o di dati personali relativi a condanne penali e a reati di cui all'art. 10 GDPR.

L'obbligatorietà del registro si estende anche agli esercizi commerciali, liberi professionisti, associazioni, fondazioni, condomini che trattino dati sanitari, dati relativi alla disabilità, dati relativi a condanne penali, reati, nonché alle organizzazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso.

La sua tenuta è quindi sostanzialmente obbligatoria per tutti i professionisti e tutte le aziende.

Per le organizzazioni con meno di 250 dipendenti, obbligate alla tenuta del registro per la natura dei dati trattati, sussistono misure di semplificazione.

La soglia di 250 dipendenti indicata nel testo normativo all'art. 30, par. 5, è utile per discernere l'obbligo di tracciare ogni tipo di trattamento dal mero obbligo di censire esclusivamente i trattamenti collegati a possibili rischi, i trattamenti non occasionali e quelli relativi a categorie particolari di dati, o relativi a condanne penali e reati.

La tenuta del registro è sinonimo di "accountability" ovvero di "responsabilizzazione" di titolari e responsabili sull'adozione di comportamenti proattivi che diano evidenza della concreta adozione di misure in applicazione del GDPR (artt. 23-25, in particolare, e l'intero Capo IV).

Titolare e responsabile

La tenuta del registro necessita di due figure: il *titolare* e il *responsabile del trattamento*. Il primo stabilisce la finalità e le modalità del trattamento, il secondo tratta i dati per conto del titolare. Su entrambi incorre l'onere di garantire la sicurezza e la tutela dei dati degli interessati.

Il registro previsto dall'art. 30 può essere di due tipi:

- registro delle attività di trattamento del titolare del trattamento (art. 30, p. 1, GDPR);
- registro delle attività di trattamento del responsabile del trattamento (art. 30, p. 2, GDPR).

Contenuto del registro

In entrambi i casi il Registro dovrà contenere:

- il codice identificativo del trattamento: utile per richiamare gli obblighi informativi successivi nei confronti degli interessati;
- la tipologia di trattamento: per specificare, in relazione a ciascuna finalità, se siano effettuate le seguenti operazioni di trattamento:
    1. raccolta;
    2. conservazione;
    3. modifica;
    4. estrazione;
    5. consultazione;
    6. uso;
    7. comunicazione;
    8. diffusione;
    9. raffronto;
    10. registrazione;
    11. organizzazione;
    12. interconnessione;
    13. limitazione;
    14. cancellazione;
    15. archiviazione;
    16. distruzione;

- le categorie dei dati per specificare quali tipi di dati vengono raccolti e trattati;
- la categoria dei destinatari a cui i dati sono riservati o saranno comunicati. Andranno riportate le categorie di appartenenza degli altri titolari a cui saranno comunicati i dati (es. Enti Previdenziali – titolare del servizio elaborazione buste paga);
- le categorie di coloro che sono interessati alla raccolta dati e quelli che sono destinatari dei medesimi. In tale campo andranno specificate sia le tipologie degli interessati (clienti, fornitori, dipendenti), sia quelle dei dati personali oggetto di trattamento (dati anagrafici, sanitari, biometrici ecc.);
- le finalità e gli scopi per cui si raccolgono i dati (statistici, profilazione dell'utente, gestione dei pagamenti ecc.). Oltre all'indicazione delle finalità del trattamento è opportuno indicare anche la base giuridica dello stesso (art. 6 GDPR), con riferimento particolare al "legittimo interesse" perseguito, le "garanzie adeguate" poste in essere e la valutazione d'impatto posta in essere dal titolare del trattamento (prov. Garante del 22/02/2018);
- nel campo "trasferimento dei dati personali verso un paese terzo o una organizzazione internazionale", l'informativa in merito ai trasferimenti attuati e l'indicazione geografica relativa al paese e al soggetto terzo ricevente;
- nel campo "termini ultimi previsti per la cancellazione delle diverse categorie di dati", l'individuazione dei tempi di cancellazione per tipologia e finalità di trattamento (per es. i dati relativi ai rapporti contrattuali saranno salvati per 10 anni in ossequio all'art. 2220 c.c.);
- nel campo "descrizione generale delle misure di sicurezza", le misure tecnico-organizzative adottate dal titolare ex art. 32 GDPR. La lista espressa nel citato art. 32 non è esaustiva e può essere integrata in base alle esigenze individuata dal titolare del trattamento;
- le tutele tecniche e organizzative che sono state adottate per prevenire i rischi di distruzione, perdita o accesso non autorizzato ai dati;

In ogni caso, è sempre possibile elevare il grado di dettaglio del registro per acquisire maggiori informazioni.

Compilazione

Il registro può essere istituito in forma cartacea o elettronica e deve indicare, con elementi certi e verificabili, la data della prima istituzione e quella dell'ultimo aggiornamento. Al suo interno debbono essere dettagliate le modalità e gli scopi del trattamento, le categorie dei dati trattati e le misure di sicurezza scelte. Il registro deve essere sempre aggiornato in tempo reale e in maniera costante; anche le variazioni adottate seguono i medesimi tempi. Qualsiasi cambiamento in ordine alle modalità, finalità, categorie dati e interessati deve essere immediatamente inserito nel registro dando conto delle modifiche intervenute.

Elemento prioritario è dato dalla possibilità di consultazione immediata del registro, a seguito dell'obbligatorio aggiornamento continuo del documento e della sua consultabilità, in caso contrario si rischiano sanzioni economiche elevate.

Registro del responsabile del trattamento

Il responsabile del trattamento dei dati per conto del titolare del trattamento tiene un registro di "tutte le categorie di attività relative al trattamento svolte per conto del titolare" (art. 30, par. 2, GDPR).

Quando il responsabile agisce per più soggetti distinti e autonomi, le informazioni di cui all'art. 30, par. 2, GDPR devono essere riportate nel registro suddiviso in sezioni ognuna per un suo diverso cliente.

La "descrizione delle categorie dei trattamenti effettuati" *ex* art. 30, par. 2, GDPR deve fare riferimento a quanto contenuto nel contratto di designazione a responsabile, che ai sensi dell'art. 28 del GDPR deve individuare la natura e le finalità di trattamento, il tipo di dati personali e le categorie oggetto di trattamento.

2.1.2 Il registro dell'amministratore di sistema

Il GDPR non prevede espressamente il ruolo dell'amministratore di sistema, voluto e definito dal Garante della Privacy (prov. 27/11/2008 mod. 26/06/2009) quale figura autonoma e operativa diversa dal Titolare del Trattamento.

L'amministratore di sistema è una persona fisica o l'ente che ha il compito di dedicarsi alla gestione e manutenzione di un sistema informatico d'impresa. A tale attività può essere incaricato un soggetto interno all'azienda; i compiti che dovrà osservare vengono indicati in un documento in maniera analitica. Qualora la scelta venga riservata a un soggetto esterno, un contratto designerà il ruolo e le funzioni ad esso attribuite.

L'intervento di questa particolare figura tecnica è necessario per occuparsi della gestione dei vari sistemi informatici presenti all'interno della rete e in particolare della workstation, notebook, server, sistemi di backup, sistemi disponibili in rete, posta elettronica, sistemi di navigazione del web e filtraggio. L'amministratore di sistema (ADS), come di seguito specificato, può dedicarsi inizialmente all'installazione di tutti i sistemi, per poi definire le configurazioni necessarie al corretto funzionamento. In seguito, il suo apporto consentirà la verifica della corretta funzionalità e gli aggiornamenti dell'hardware e del software in caso di avarie.

I compiti dell'amministratore di sistema

All'ADS, solitamente scelto tra i professionisti informatici, sono attribuiti i seguenti compiti:

- classificare analiticamente le banche dati e attuare politiche di sicurezza a tutela dei dati personali,
- individuare i soggetti incaricati della custodia delle credenziali per l'accesso al sistema informatico e vigilare sulla loro attività,
- impostare e gestire un sistema di autentificazione informatica del trattamento dei dati personali,
- adottare un sistema idoneo alla registrazione degli accessi logici,
- assicurare e gestire sistemi di salvataggio e ripristino dei dati (backup e recovery) anche automatici e approntare adeguate misure di salvaguardia dei dati personali (es. antivirus),

- impartire a tutti gli incaricati adeguate istruzioni tecnico/organizzative per utilizzare validi sistemi di salvataggio dei dati,
- adottare sistemi per la custodia delle copie di sicurezza dei dati,
- predisporre un piano di controlli periodici per verificare l'efficacia delle misure di sicurezza.

Il provvedimento del Garante prevede per l'ADS l'obbligo di registrazione con completezza degli accessi logici (access log) sia server che client. La finalità di tali registrazioni è quella di poter verificare le anomalie nella frequenza degli accessi e nelle loro modalità.

Le registrazioni eseguite devono comprendere i riferimenti temporali, l'attinenza all'evento che le ha generate e devono essere conservate per almeno sei mesi.

Registrazione degli accessi

Devono essere adottati sistemi adeguati a registrare gli accessi logici (ovvero le autenticazioni informatiche) effettuati dall'amministratore di sistema ai sistemi di elaborazione e agli archivi elettronici.

Questi log di accesso devono essere completi, non modificabili e verificabili nella loro integrità, in modo da garantire un controllo efficace e coerente con le finalità di verifica per cui sono stati predisposti.

Anche i *client*, intesi come "postazioni di lavoro informatizzate", sono compresi tra i sistemi per cui devono essere registrati gli accessi da parte dell'ADS.

Per "access log" si intende la registrazione degli eventi generati dal sistema di autentificazione informatica all'atto dell'accesso o al tentativo di accesso da parte di un amministratore di sistema o alla sua disconnessione dai collegamenti interattivi a sistemi di elaborazione o di software.

2.1.3 Il registro delle violazioni - "data breach"

La violazione dei dati personali

La violazione dei dati personali commessa per negligenza o dolo comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; può compromettere i dati trattati, mettendo a rischio uno o più dei tre principi della sicurezza delle informazioni: la riservatezza, l'integrità o la disponibilità degli stessi. Gli esempi più eclatanti risultano:

- l'accesso o l'acquisizione dei dati da parte di soggetti non autorizzati,
- il furto o la perdita di dispositivi informatici che contengono i dati sensibili,
- l'impossibilità di accedere alla consultazione dei dati per fatti accidentali o per attacchi esterni virus, malware, ecc.,
- la perdita per cause incidentali, eventi avversi, incendi, inondazioni,
- la divulgazione dei dati non autorizzata.

Il titolare del trattamento, senza incorrere in ritardi, possibilmente entro 72 ore dalla scoperta, deve

notificare la violazione dei dati personali riscontrata al Garante della Privacy. Qualora l'infrazione venga giudicata come rispondente ad un elevato rischio per i diritti alle persone, il titolare ha l'obbligo di informare tutti i soggetti interessati, utilizzando validi canali di comunicazione.

L'inosservanza al diritto alla privacy, mediante fatti concludenti a danno di terzi soggetti, deve essere documentata, per rilevare le violazioni perpetrate, mediante l'istituzione e trascrizione su un apposito registro. Tale documentazione e le relative annotazioni sul Data Breach formano un obbligo per il titolare, al fine di consentire all'Autorità di effettuare eventuali verifiche, rispetto all'osservanza della norma in caso di violazioni subite.

Disposizioni UE e del Garante

Il GDPR e in particolare le linee guida WP 250 impongono al titolare del trattamento di creare un registro interno delle violazioni, previsto obbligatoriamente dal Garante.

Il titolare determina autonomamente con quale metodo e strumenti la struttura deve documentare i dettagli della possibile violazione, comprese le cause, i fatti e i dati personali degli interessati. A coronamento del buon esito della registrazione è necessario indicare gli effetti e le conseguenze della violazione, unitamente ai provvedimenti necessari, intrapresi e adottati, per porvi rimedio.

Conservazione della documentazione

Il GDPR non stabilisce una durata precisa per la conservazione della documentazione: spetta al Titolare del Trattamento definire i tempi, in base alle finalità del trattamento e ai principi di necessità e proporzionalità. Il principio di responsabilità implica la necessità di stabilire un termine entro il quale l'autorità di controllo possa avviare l'istruttoria relativa a una specifica violazione, nonché un ulteriore periodo entro cui possa richiedere la documentazione pertinente.

Il titolare e il responsabile del trattamento debbono individuare e disporre di una procedura informatizzata che in presenza di una violazione valuti il rischio, come porvi rimedio e assicurare la notifica ai soggetti che hanno subito la violazione.

La mancata conservazione della corretta documentazione relativa ad una violazione riscontrata può comportare attività sanzionatoria da parte dell'autorità di controllo ai sensi dell'art. 58 GDPR e l'elevazione della sanzione amministrativa prevista dall'art. 83 GDPR.

Il registro dovrà, inoltre, essere strutturato in modo da garantire l'integrità e la tracciabilità delle registrazioni in esso contenute.

Contenuto del registro

Con il Provvedimento n. 161 del 4 aprile 2013, in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali, il Garante ha anche fornito alcune indicazioni al titolare del trattamento in merito ai contenuti e alle caratteristiche del registro dei *data breach*:

- i dettagli relativi alle violazioni comprese le informazioni inerenti, le cause, il luogo ove è avvenuta la tipologia e i dati personali violati;
- gli effetti e le conseguenze della violazione;
- il piano d'intervento predisposto dal titolare;
- le motivazioni delle decisioni assunte nei casi in cui: 1) il titolare ha deciso di non procedere alla notifica, 2) il titolare ha ritardato nella procedura di notifica, 3) il titolare ha deciso di non notificare la violazione agli interessati.

2.1.4 Il registro della formazione

Formazione privacy

Elemento fondamentale, previsto dalle norme che regolano la materia della privacy nelle aziende e nelle pubbliche amministrazioni, è la costante e adeguata formazione di tutti i soggetti che, a vario titolo, si occupano degli adempimenti per la tutela dei dati personali.

Il GDPR ha introdotto il vincolo della formazione, rendendola una misura di sicurezza obbligatoria per tutti, dipendenti e collaboratori, non solo per le figure specializzate.

La mancata formazione è considerata una violazione di legge e, come tale, in mancanza è soggetta a una sanzione amministrativa, prevista dall' art. 83 comma 4 del GDPR, pari al 2% del fatturato di gruppo sino ad un massimo di 10 milioni di euro.

Il piano di formazione privacy

In base al modello organizzativo e alla specifica realtà dell'impresa, si dovrà verificare in che modo i compiti inerenti alla privacy siano distribuiti all'interno dell'azienda. Verificate le dimensioni e il numero degli operatori autorizzati a trattare i dati ai vari livelli, sarà necessario e obbligatorio, in adempimento alle norme GDPR, attuare un piano di formazione specifica.

La formazione generica è necessaria per coloro che si occupano di trattamento dei dati (normativa di riferimento e adempimenti); per i referenti e le figure dotate di responsabilità serve, invece, una formazione GDPR specifica. Nella fase iniziale occorre verificare il grado di formazione base delle varie categorie di operatori e il livello di competenze raggiunto. Successivamente, si imposta la formazione mediante corsi di didattica, con vari gradi di informazione, al fine di migliorare il livello di consapevolezza e di conoscenza degli addetti che prendono parte ai corsi.

In ottica di *accountability* risulta fondamentale verificare, dopo l'istituzione di corsi specialistici, erogati da professionisti esperti della materia, il grado di conoscenza sulle diverse tematiche affrontate da parte delle singole aree aziendali interessate alla formazione.

Il registro della formazione

L'attività didattica e formativa, quale misura di prevenzione per controllare il rischio di violare i diritti degli interessati, si chiude necessariamente con una verifica dell'apprendimento.
I temi trattati riguardano principalmente:

- il GDPR e le sue indicazioni principali;
- i soggetti individuati dal GDPR;
- i principi alla base del trattamento dei dati;
- i principali adempimenti previsti dal GDPR;
- i diritti degli interessati;
- l'Autorità di controllo;
- le sanzioni.

È opportuno che la formazione sia documentata mediante la tenuta di un apposito registro.

Questo strumento aziendale è oltremodo utile per certificare:

- il soggetto che ha effettuato il corso di formazione;
- il periodo in cui è stato erogato il corso;
- le materie trattate;
- gli operatori che a vario livello hanno frequentato i corsi di formazione;
- i risultati della verifica finale a cui sono stati sottoposti gli operatori.

Detto registro risulta utile e fondamentale per dimostrare alle Autorità Europee e al Garante di aver adempiuto alla formazione obbligatoria; per l'azienda costituisce un valido riscontro della specificità dei corsi resi agli addetti alla privacy e dell'esito dei test superati da ogni corsista.

2.1.5 Il registro dei *penetration test* (pen)

Risulta molto utile per le organizzazioni eseguire attacchi informatici simulati per testare i punti di forza e di debolezza dei propri sistemi di sicurezza, al fine di aggiornare, ove risulti necessario in base all'esito dei test, le soluzioni adottate in materia di sicurezza informatica, riducendo al minimo le proprie vulnerabilità e, quindi, la possibilità di successo di eventuali attacchi.

I PT o PEN, come misura proattiva di sicurezza informatica, vengono eseguiti utilizzando le strategie e le tecniche degli attaccanti, per valutare la "*hackability*" dei sistemi informatici, della rete o delle applicazioni web di un'organizzazione, identificarne i rischi e mitigarli prima che vengano sfruttati.

Oltre a report dettagliati relativi alle singole fasi dei test, riconducibili a: raccolta delle informazioni (*information gathering*), scansione della rete (*network scanning*), enumerazione (*enumeration)*, ricerca vulnerabilità (*vulnerability assessment*), accesso al sistema (*exploitation*), mantenimento dell' accesso al sistema (*post exploitation*)e report finale (final report), sarebbe utile mantenere un apposito registro,

riepilogativo delle simulazioni effettuate, con la specifica degli strumenti utilizzati e dei relativi risultati.

2.1.6 Il registro dei *disaster recovery*

In una realtà in cui tutto è collegato alle tecnologie digitali, ancora prima di avere l'obbligo di garantire la protezione dei dati trattati, per le organizzazioni è di primaria importanza essere in grado di ripristinare, in temi ridottissimi, i sistemi critici a seguito di un'interruzione, al fine di garantire la *business continuity*.

Per adempiere agli obblighi di cui al GDPR, oltre che per le finalità di riduzione degli impatti economici delle interruzioni di business, le organizzazioni dovranno dotarsi di un Piano di DR (*Disaster Recovery*), che includa istruzioni dettagliate su come rispondere a tutti gli incidenti (non esclusivamente agli attacchi informatici) che generino danneggiamenti, perdite, furti, diffusione non autorizzata dei dati trattati, a tutela dei diritti degli interessati. Come per i *Penetration Test*, è importante tenere traccia, in un apposito registro, delle simulazioni di ripristino periodicamente effettuate.

2.1.7 Il registro dei sub responsabili del trattamento

Ai sensi dell'art. 28 del GDPR, qualora il trattamento dei dati venga effettuato da soggetti diversi dal titolare del trattamento, ciò deve avvenire previa autorizzazione scritta da parte del titolare e a fronte di un contratto o altro atto giuridico, che lo disciplini dettagliatamente, prevedendone la materia, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, nonché tutte le condizioni previste dal titolare.

Il registro, obbligatorio ai sensi dell'art. 30 del GDPR, riporta le predette informazioni, relativamente ai Sub Responsabili (o responsabili esterni del trattamento) autorizzati e, parallelamente, tiene traccia anche delle nomine ricevute quali Responsabili Esterni (o Sub Responsabili), da parte di soggetti esterni all'organizzazione.

2.1.8 Il registro dell'esercizio dei diritti da parte degli interessati

L'esercizio dei diritti da parte degli interessati

I diritti dell'interessato sono disciplinati dagli artt. 7, 15, 16, 17, 18, 19, 20, 21, 77 del GDPR.

I diritti esercitabili dall'interessato sono:

1. diritto all'informazione (diritto di ottenere informazioni su quali dati siano trattati dal titolare e il criterio alla base del trattamento);
2. diritto di accesso (diritto di chiedere e ottenere in forma intellegibile i dati in possesso del titolare e di richiederne copie);
3. diritto alla rettifica (diritto di chiedere modifiche e/o aggiornamenti);
4. diritto di cancellazione (diritto di ottenere la cancellazione dei dati in possesso del titolare);

5. diritto di opporsi (esercitare l'opposizione al trattamento in tutto o in parte);
6. diritto di revoca del consenso (diritto di revocare il consenso al trattamento dei dati in qualsiasi momento);
7. diritto di opporsi al trattamento automatizzato (non essere assoggettati a trattamenti basati esclusivamente su decisioni automatizzate, compresa la profilazione);
8. diritto all'oblio (diritto di chiedere e ottenere trasformazione in forma anonima o alla cancellazione dei dati);
9. diritto di chiedere e ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento;
10. diritto alla portabilità dei dati (possibilità di chiedere il trasferimento dei propri dati personali);
11. diritto di proporre reclamo all'autorità di controllo.

Le richieste di esercizio dei diritti da parte degli interessati vanno gestite dall'organizzazione e sarebbe utile tenerne traccia in un apposito registro.

Contenuto del registro

Il Registro dovrebbe contenere, in ordine cronologico, le richieste di esercizio di diritti ricevute dagli interessati, con i relativi dettagli sulle richieste e sulle modalità di gestione delle stesse.

2.1.9 Il registro dei visitatori e la protezione della privacy

Esigenza di monitorare i flussi dei visitatori

Molte aziende di medie e grandi dimensioni hanno la necessità costante di monitorare le presenze dei visitatori, in entrata e in uscita, dagli uffici e dallo stabilimento. Questo avviene principalmente per i seguenti motivi:

- regolamentazione degli accessi.

La presenza di un registro prevede che solo le persone autorizzate abbiano accesso alla struttura.

- Miglioramento della sicurezza.

La registrazione delle informazioni dei visitatori consente di conoscere in ogni momento le presenze nell'azienda anche in caso di emergenza e riduce il rischio di intrusioni non desiderate.

- Conformità alla normativa vigente.

Particolarmente in alcuni settori, quali quello sanitario, della finanza e anche nel settore alimentare per l'attuazione di politiche di *food defence,* esistono normative stringenti e specifiche che richiedono la registrazione dei visitatori. L'adozione del registro presenza aiuta a tale scopo.

- Gestione delle risorse.

L'adozione di un registro digitale delle presenze aiuta a gestire meglio gli spazi aziendali, come le stanze per gli incontri e le aree espositive dedicate ai clienti.

- Efficienza nell'accoglienza.

Con il registro in uso l'accoglienza dei visitatori diventa più efficiente e le informazioni vengono registrate rapidamente creando un'impressone positiva.

- Analisi dei dati.

L'archivio che si forma con le registrazioni consente di analizzare le visite e ottimizzare le operazioni conseguenti.

L'azienda può istituire con successo il registro adottando software specifici o app personalizzate. Tali sistemi consentono di disporre di dati storici utilizzabili per particolari scelte aziendali e per inviare specifiche notifiche agli ospiti, interagendo anche con i sistemi di sicurezza esistenti.

L'ulteriore finalità che giustifica l'adozione del registro consiste nel mantenere un riscontro della presenza di esterni ai fini della raccolta di informazioni, come ad esempio: la presenza in azienda di manutentori incaricati di operare attività programmate. È possibile anche verificare che le prestazioni di tali artigiani siano attestate da rapporti d'intervento. Ulteriore riscontro è possibile per le prestazioni di qualsiasi professionista e della sua reale presenza in azienda, prima di erogare il pagamento delle prestazioni rese.

Tenuta del registro dei visitatori

Per la tenuta del registro, su supporti cartacei o tramite soluzioni elettroniche, vengono acquisiti di solito i seguenti dati:

- nome e cognome del visitatore – il ruolo – la società di appartenenza - la funzione – la persona con la quale deve incontrarsi – la data e l'orario d'ingresso – l'orario di uscita – quando previsto il numero di badge – in molti casi la firma in entrata e in uscita – talvolta la verifica dell'identità del visitatore tramite un documento.

La firma, se si utilizza un registro in formato elettronico, può essere acquisita in formato digitale o anche facendo ricorso "alla firma elettronica semplice" come definita dal Regolamento eIDAS (Electronic Identification Authentication and Signature) – Regolamento UE n. 910/2014 sull'identità digitale, che identifica tre tipologie di firma elettronica: semplice, avanzata e qualificata.

Criticità nella tenuta e conservazione dei dati

I dati acquisiti sul registro delle presenze dovrebbero essere conservati per un tempo limitato ad alcuni giorni. La tendenza di alcuni imprenditori è quella di mantenere in vita i dati incamerati nel computer per formare un archivio storico da far valere quale prova dell'attività svolte da terzi soggetti, a fronte di possibili controlli e verifiche degli organismi preposti.

Tale prassi diventa oltremodo rischiosa quando vengono archiviati dati particolari quali la firma digitalizzata, copia del documento d'identità, elementi necessari per la restituzione del badge attinente

alla security aziendale. Il grado di protezione dei dati si eleva quando vengono acquisite notizie personali del visitatore in tema sanitario o finanziario.

Quando i dati vengono archiviati corre l'obbligo di un'adeguata informativa per i visitatori.

La presenza del registro dei visitatori comporta necessariamente l'aggiornamento del registro dei trattamenti, l'individuazione a priori dei tempi di conservazione, la nomina di un responsabile della gestione e archiviazione dei dati e della funzione incaricata alla distruzione del registro cartaceo o allo svuotamento dei file informatici.

Si allegano alcuni format da utilizzare come base per la predisposizione dei succitati registri (*Allegato 2*).

2.2. Le informative ai sensi dell'art. 13 del GDPR

Agli artt. 13 e ss. del GDPR sono indicate tutte le informazioni che il Titolare del trattamento è tenuto a fornire all'interessato nel momento in cui procede con la raccolta dei suoi dati personali, sia che questa raccolta avvenga presso l'interessato, sia qualora i dati personali non siano stati ottenuti dall'interessato.

Ogni informativa dovrà contenere le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

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

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'art. 46 o 47, o all'art. 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

1. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per

determinare tale periodo;

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

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

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

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

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 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 il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

3. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni. Ai fini dell'audit di valutazione della conformità, l'auditor dovrà verificare:

1. la presenza delle informative necessarie;
2. la correttezza formale delle stesse, in termini di contenuti obbligatori previsti;
3. l'avvenuta trasmissione ai soggetti interessati (es. clienti, fornitori, dipendenti, candidati all'assunzione, ecc.);
4. l'esistenza di un processo di riesame periodico e di monitoraggio, che garantisca l'assolvimento dell'obbligo, in relazione ai nuovi ingressi e alle eventuali modifiche organizzative (nuovi fornitori, clienti, dipendenti, ecc.).

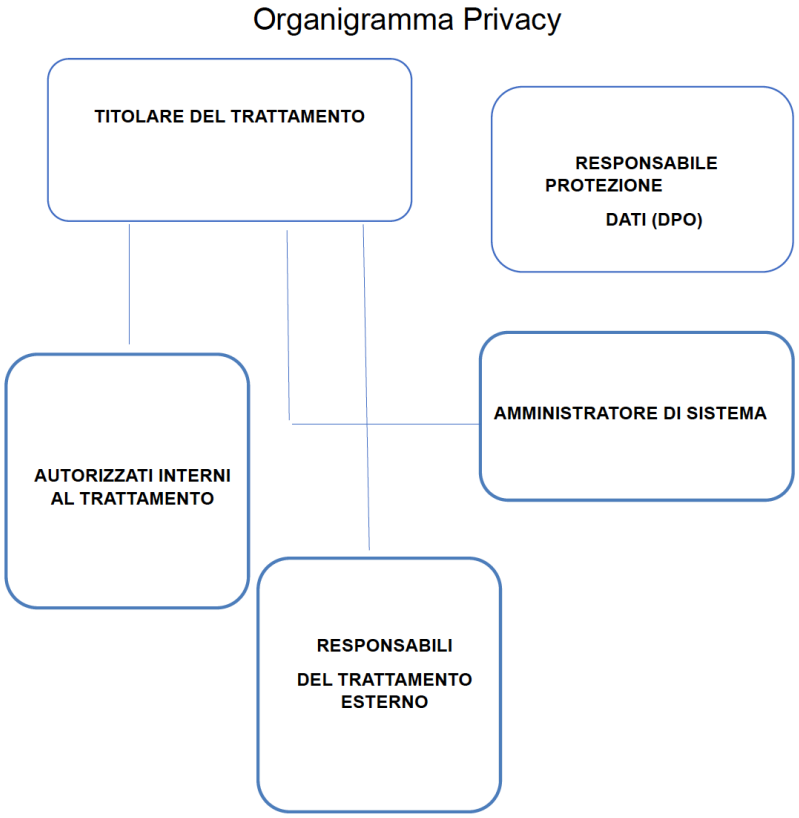
2.3. L'organigramma e le nomine degli attori della privacy

Il primo adempimento che un'organizzazione dovrebbe espletare, in sede di adeguamento alla normativa sulla protezione dei dati, è sicuramente l'individuazione, all'interno dell'organizzazione, degli "attori" della privacy, ovvero delle figure, indicate dal GDPR, preposte all'assolvimento di particolari compiti in materia. L'auditor acquisirà, quindi, come informazione documentata l'organigramma

privacy e dovrà, soprattutto, verificare se tali figure con i rispettivi ruoli siano stati regolamentati da opportune nomine.

Le principali figure sono sintetizzabili in:

- titolare del trattamento;
- eventuali Contitolari;
- responsabili del trattamento esterno o subresponsabili;
- soggetti autorizzati al trattamento dei dati personali;
- amministratore di Sistema;
- eventuale Data Protection Officer (DPO).



In allegato si riportano alcuni esempi di nomine formali (*Allegato 3*).

2.4. Le altre informazioni documentate: l'analisi dei rischi e la DPIA

Durante la conduzione dell'audit, il professionista dovrà verificare che l'organizzazione abbia mappato tutte le attività svolte, ovvero i processi primari e quelli di supporto necessari per il raggiungimento

degli obiettivi aziendali e abbia effettuato l'Analisi dei rischi prevista dal GDPR, onde individuare, a fronte dei rischi di perdita, furto e diffusione dei dati trattati, le necessarie contromisure da adottare per prevenire il verificarsi di tali eventi. La valutazione sui rischi per i diritti e le libertà delle persone fisiche viene citata in diversi articoli del GDPR, ma in particolare l'art. 24 recita:

1. *Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.*

Così come evidenziato dall'art. 25 "Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita", le misure progettate e realizzate devono assicurare un adeguato livello di sicurezza bilanciando da un lato, lo stato dell'arte e i costi di attuazione e, dall'altro, i rischi che presentano i trattamenti relativi alla natura dei dati personali da proteggere.

La normativa non fornisce un'indicazione perentoria circa le misure di sicurezza da adottare, ma solo un elenco esemplificativo di misure che possono essere adottate dal titolare del trattamento sulla base delle risultanze dell'analisi dei rischi condotta, tra cui:

- pseudonimizzazione e cifratura dei dati personali;
- capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- esistenza di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare poi il livello di adeguatezza delle misure adottate, ai sensi dell'art. 32 del GDPR, andrà verificato se le stesse siano effettivamente in grado di prevenire e contrastare i rischi derivanti dall'attività di trattamento, ossia distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

I principali approcci con cui il titolare può provvedere all'analisi dei rischi sono richiamati dall'Autorità Garante Italiana, tramite il portale dedicato ENISA.EUROPA.EU.

Nel portale si trovano strumenti a disposizione delle aziende per valutare la sicurezza del trattamento dei dati personali.

Ulteriori metodologie disponibili sono quelle offerte dalle altre Autorità di controllo, quali ad esempio l'*Agencia Española de Protección de Datos* (AEPD), o l'Autorità Garante Francese, *Commission Nationale de l'informatique et des libertés* (CNIL).

Un altro adempimento da verificare, quando ne ricorrano i presupposti, è la redazione della DPIA.

Il comma 7 dell'art. 35 del GDPR prevede che la DPIA contenga almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Sinteticamente la DPIA consente di verificare il rispetto dei principi fondamentali rispetto al trattamento, cioè quelli inerenti:

- finalità;
- basi legali;
- adeguatezza dei dati;
- esattezza dei dati;
- periodo di conservazione;
- informativa;
- raccolta del consenso;
- diritto di accesso e diritto alla portabilità dei dati;
- diritto di rettifica e diritto di cancellazione;
- diritto di limitazione e diritto di opposizione;
- responsabili del trattamento;
- trasferimento dei dati;

e il rispetto delle misure esistenti o pianificate (in pratica le misure di sicurezza a fronte del rischio di accesso illegittimo ai dati, modifiche indesiderate dei dati, perdite dei dati) quali il controllo degli accessi logici, tracciabilità, archiviazione, vulnerabilità, backup, manutenzione, gestione, protezione da fonti di rischio non umane, gestione del personale, vigilanza sulla protezione dei dati.

A fronte del risultato della DPIA, in caso di livello di rischio rilevato occorrerà eventualmente mettere in atto ulteriori misure, oltre quelle esistenti, finalizzate a mitigare il rischio stesso.

La norma facoltativa più utilizzata relativamente alla predisposizione della DPIA è rappresentata dalla ISO/IEC 29134, inizialmente pubblicata nel 2011 e aggiornata nel 2017, nella quale viene considerato in particolare l'aspetto relativo ai rischi tecnici e alla vulnerabilità del trattamento. Preliminarmente occorre individuare se il tipo di trattamento renda obbligatoria l'elaborazione di una DPIA (vedasi l'elenco delle tipologie di trattamento soggetti alla valutazione di impatto individuate dal Garante), pur

essendo comunque consigliabile effettuare tale valutazione.

In alternativa il Garante Francese ha reso disponibile un software anche in lingua italiana, grazie alla collaborazione tra i Garanti francese e italiano, che può essere installato gratuitamente per procedere alla redazione della DPIA. (vedasi anche il doc. web 8581268 del Garante).

Il risultato della DPIA **non accettabile** comporta il fatto di dover riesaminare più compiutamente i rischi e individuare nuove misure maggiormente idonee a garantire la sicurezza dei dati personali, rielaborare quindi la DPIA fino a giungere al risultato di DPIA accettabile.

Il risultato della DPIA **accettabile ma migliorabile** comporta il fatto di dover riesaminare più compiutamente i rischi e individuare misure correttive a quelle già individuate maggiormente idonee a garantire la sicurezza dei dati personali.

Il risultato della DPIA **accettabile** significa che le informazioni fornite sono sufficienti e che le modalità di trattamento sono ottimali e comportano la conformità del trattamento medesimo (circa la nozione di accettabile si veda l'allegato 2 alle linee guida WP248).

Lo scopo dell'audit sarà di valutare anche se l'organizzazione abbia messo in atto le azioni conseguenti agli esiti della valutazione.

Ai fini della raccolta delle evidenze documentali durante la conduzione dell'audit, si riporta un elenco non esaustivo della documentazione da richiedere. Sono esclusi i riferimenti alle misure tecniche, che saranno trattate nel capitolo terzo.

CHECK LIST PRELIMINARE PER CONFORMITÀ DOCUMENTALE
ORGANIGRAMMA
NOMINE: - DPO - SOGGETTI AUTORIZZATI AL TRATTAMENTO - AMMINISTRATORE DI SISTEMA - RESPONSABILI ESTERNI - SUB RESPONSABILI
AMBITI DI TRATTAMENTO
ISTRUZIONI OPERATIVE
INFORMATIVE: - CLIENTI - FORNITORI - DIPENDENTI - CANDITATI ALL'ASSUNZIONE

- VIDEOSORVEGLIANZA - SITO WEB
PROCEDURA DATA BREACH
REGISTRO DEI TRATTAMENTI DEL TITOLARE E/O DEL RESPONSABILE INTERNO
REGISTRO DELL'AMMINISTRATORE DI SISTEMA
REGISTRO DELLA FORMAZIONE
REGISTRO DEI DATA BREACH
REGISTRO DEI PENETRATION TEST
REGISTRO DEI DISASTER RECOVERY
REGISTRO DEI SUB RESPONSABILI
REGISTRO DELL'ESERCIZIO DEI DIRITTI
REGISTRO DEI VISITATORI
ANALISI DEI RISCHI
DPIA

Capitolo terzo

LE MISURE TECNICHE DI SICUREZZA

3.1. Un utile riferimento: l'Annex A della norma ISO/IEC 27001:2022

La norma 27001 è divisa in due parti separate, di cui la prima composta da 11 clausole (dalla 0 alla 10), che descrivono i requisiti della ISO 27001 che sono obbligatori se l'azienda vuole essere conforme alla norma e conseguire la certificazione, ma sono anche molto utili a fini non certificativi, per la conformità alla normativa cogente. La seconda parte, Annex A (o Allegato A), è una linea guida per i 114 obiettivi di controllo e per i controlli da effettuare, ovvero integra le clausole e i loro requisiti con un elenco di controlli selezionati a valle del *Risk Assesment* effettuato. Si tratta, in pratica, di indicazioni specifiche sulle misure di sicurezza informatica da implementare.

Anche questa parte si ritiene di grande utilità per le organizzazioni che intendano perseguire una politica di sicurezza dei dati e di conformità al GDPR.

In allegato si riportano le tabelle riguardanti l'elenco dei controlli previsti dall'Annex A e alcuni esempi di evidenze da reperire durante un audit di verifica della conformità, ove applicabili alla specifica organizzazione (*Allegato 4*).

Segue un elenco di *policies* aziendali che andrebbero adottate in risposta alle contromisure richieste dall'Annex A e che l'auditor, a seconda delle situazioni specifiche, dovrebbe trovare almeno in parte implementate presso l'organizzazione.

POLICY N.	DESCRIZIONE POLICY
POL-1	*Politica uso accettabile*
POL-2	*Politica controllo accessi*
POL-3	*Politica gestione asset*
POL-4	*Politica conservazione documenti digitali*
POL-5	*Politica di gestione dei documenti*
POL-6	*Politica di crittografia*
POL-7	*Politica di backup e ripristino dei dati*
POL-8	*Politica di classificazione e trattamento informazioni*
POL-9	*Politica di utilizzo internet e posta elettronica*

POL-10	*Politica per le password*
POL-11	*Politica di dismissione delle regitrazioni*
POL-12	*Politica di scansione e smaltimento documentazione*
POL-13	*Politica di protezione della scrivania*
POL-14	*Politica di protezione delle email*
POL-15	*Politica di gestione degli incidenti di sicurezza*
POL-16	*Politica di sicurezza dei server*
POL-17	*Politica di connessione di terze parti*
POL-18	*Politica di rete wireless*
POL-19	*Politica di gestione dei supporti di memorizzazione*
POL-20	*Politica di sicurezza per il pc*
POL-21	*Politica di smaltimento delle apparecchiature*
POL-22	*Politica di sviluppo e manutenzione dei sistemi*
POL-23	*Politica di progettazione e sviluppo sicuro*
POL-24	*Politica di sicurezza per laptop e dispositivi mobili*
POL-25	*Politica per software malevolo e antivirus*
POL-26	*Politica per il telefono cellulare*
POL-27	*Politica per le infrastrutture fisiche ed ambientali*
POL-28	*Politica di valutazione dei record*
POL-29	*Politica di telelavoro*
POL-30	*Politica di segnalazione e gestione degli incidenti*
POL-31	*Politica di sicurezza per i fornitori*
POL-32	*Politica di data masking*
POL-33	*Politica di oblio*
POL-34	*Politica di gestione della capacita'*
POL-35	*Politica di gestione della configurazione*
POL-36	*Politica di gestione dei log file*
POL-37	*Politica di bring your own device (byod)*

Capitolo quarto

LA DIRETTIVA UE 2022/2555 (NIS2)

4.1. La Direttiva

La Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, cd. NIS 2, ha come ambito la Cybersecurity e la resilienza dei servizi essenziali e digitali, con l'obiettivo di rafforzare la sicurezza delle reti e dei sistemi informativi degli Stati membri e quindi dell'Unione Europea. Vengono riportati di seguito, in modo schematico, i tratti essenziali e i principali adempimenti della Direttiva, per la stretta connessione con le tematiche trattate, con riferimento all'obbligo di adozione di misure di sicurezza informatica di cui al GDPR. La Direttiva costituisce, infatti, un obbligo per tutti i soggetti indicati come destinatari della normativa, ma può essere anche un utile riferimento per le organizzazioni che intendano implementare solide misure di Cybersecurity, nell'ottica del pieno adempimento al GDPR.

4.1.1 Finalità, ambito di applicazione, obblighi dei soggetti interessati

La Direttiva NIS 2 mira a:

- aumentare la **resilienza informatica** degli operatori critici;
- migliorare la **cooperazione tra Stati membri** per la gestione di crisi cyber;
- assicurare un **livello minimo armonizzato** di misure di sicurezza in tutta l'UE;
- estendere l'ambito rispetto alla Direttiva NIS 1 (del 2016), includendo più settori e soggetti.

NIS 2 Coinvolge due categorie di soggetti:

a) Enti essenziali (art. 3)

- Energia, trasporti, sanità, acqua potabile, PA centrale, finanza, infrastrutture digitali

b) Enti importanti

- Manifatturiero critico, fornitori ICT, data center, ricerca, servizi postali, PA locale

L'applicazione della NIS 2 è automatica per enti con più di **50 dipendenti** o con **fatturato maggiore di € 10** milioni.

<u>Principali obblighi per i soggetti interessati</u>

Misure di gestione del rischio (art. 21)

I soggetti devono adottare:

- politiche di sicurezza e gestione degli incidenti;
- continuità operativa e disaster recovery;
- sicurezza nella supply chain;
- autenticazione a più fattori;
- formazione periodica;
- sicurezza nelle acquisizioni e nello sviluppo del software.

Obblighi di notifica degli incidenti (art. 23)

- notifica preliminare all'autorità **entro 24 ore**;
- relazione intermedia (se richiesto);
- relazione finale **entro 72 ore – 1 mese**;

L'obbligo si estende agli **incidenti significativi**, anche non data breach.

Governance e responsabilità

- I dirigenti sono **direttamente responsabili** della conformità;
- Le organizzazioni devono garantire supervisione e rendicontazione interna.

4.1.2 Coordinamento con altri regolamenti – Ruoli e Autorità coinvolte

Normativa	Rilevanza
GDPR	Prevede l'obbligo di notifica dei data breach (entro 72h) art. 32
AI Act	I sistemi critici ad alto rischio devono garantire resilienza e sicurezza informatica
DORA	È specifico per il settore finanziario; prevede delle norme più dettagliate sulla resilienza digitale

Le Autorità coinvolte sono:

- Autorità competente nazionale (es. in Italia: ACN – Agenzia per la Cybersicurezza Nazionale)
- CSIRT (Computer Security Incident Response Team)
- Cooperazione europea tramite il network CyCLONe e ENISA

Le sanzioni sono previste in modo **proporzionato e con intento dissuasivo**, similmente a quanto previsto dal GDPR:

- Enti essenziali: fino a **€10 milioni** o **2% del fatturato globale annuo**;
- Enti importanti: fino a **€7 milioni** o **1,4% del fatturato**;
- Possibilità di sanzioni amministrative per **manager responsabili** in caso di negligenza grave.

4.1.3 Gli adempimenti

Sinteticamente le organizzazioni sono tenute a:

- verificare in primis se si è soggetto pertinente NIS 2 (essenziale o importante);
- effettuare la nomina di un referente per la sicurezza o CISO;
- eseguire una valutazione dei rischi informatici;
- adottare politiche di sicurezza e un piano di risposta agli incidenti;
- implementare almeno le misure tecniche minime obbligatorie;
- integrare i processi di notifica con quelli GDPR e privacy;
- formare regolarmente il personale (compresi i dirigenti);
- organizzare audit periodici e test di resilienza;
- aggiornare la documentazione interna: policy, registri, report;
- interagire con l'Autorità nazionale (ACN) per dubbi o notifiche.

4.1.3.1 Checklist di conformità – NIS 2

Di seguito sono riportati gli adempimenti da verificare e che possono essere inseriti in un'apposita check list da utilizzare per gli audit. Per semplificare, sono stati suddivisi per area:

<u>Ambito e identificazione</u>

- L'Organizzazione è un **ente essenziale** o **importante**?
- L'Organizzazione è soggetta a NIS 2 per dimensioni o settore critico?
- L'Organizzazione ha ricevuto una notifica dall'autorità competente?

<u>Governance e responsabilità</u>

- È stato nominato un **responsabile sicurezza** (CISO o equivalente)
- Il board è informato e responsabilizzato
- Esiste un piano di gestione del rischio informatico
- Esistono idonee procedure di business continuity e disaster recovery

<u>Misure tecniche minime (art. 21)</u>

- Esistono policy di cybersecurity e di gestione vulnerabilità
- È attivo il logging e il monitoraggio continuo dei sistemi
- Sono in essere controlli di accesso (MFA, IAM)
- È attiva la criptografia e la protezione dati

- Vengono effettuati e testati Backup regolari
- Sono attivi Antivirus e protezioni antimalware
- Viene effettuata la formazione continua del personale

Gestione incidenti e notifica

- Esiste un processo interno per la rilevazione e gestione degli incidenti
- Esiste un processo per la gestione della prima notifica **entro 24h** all'autorità nazionale
- Esiste un processo per effettuare la relazione finale **entro 72h o max 1 mese**
- Esiste un processo per il coordinamento **NIS 2 Garante Privacy** in caso di data breach

Supply chain e fornitori

- Viene effettuata la valutazione del rischio dei fornitori terzi
- Sono stipulati contratti con idonee clausole cyber e audit
- Esistono Procedure per la gestione degli incidenti in outsourcing

Formazione e cultura aziendale

- È stato stilato un adeguato piano annuale di formazione cybersecurity
- Vengono effettuate esercitazioni simulate di incident response
- Viene mantenuta la documentazione delle attività formative

Audit e miglioramento

- Sono programmati Audit periodici (interni o esterni)
- Viene mantenuto un registro degli incidenti e delle azioni correttive attuate
- Le misure di sicurezza sono riesaminate almeno annualmente

Capitolo quinto

AI E PRIVACY: L'ARTIFICIAL INTELLIGENCE ACT

5.1. Contesto generale dell'AI Act

L'introduzione di nuovi sistemi informatici avanzati conduce alla necessità di normare, in linea con il GDPR, tutti gli applicativi che si avvalgono di sistemi basati sull'Intelligenza Artificiale (AI).

L'Intelligenza Artificiale pone l'attenzione sulla capacità di una macchina di poter eseguire compiti che richiedono aspetti propriamente caratterizzanti l'intelligenza umana, ossia il ragionamento, l'apprendimento la capacità di pianificare le attività e aspetti legati alla creatività.

L'AI coinvolge una moltitudine di tecniche poiché l'obiettivo è quello di creare sistemi informatici in grado di svolgere compiti tipici dell'intelligenza umana, come problem solving, riconoscimento di immagini, comprensione e riproduzione di linguaggio umano.

Per svolgere queste attività, quindi per poter "addestrare" questi sistemi, si sfruttano enormi quantità di dati. È facile così individuare le implicazioni a livello di Personal Data Protection che ne derivano.

Il Regolamento (UE) 2024/1689 (c.d. **Artificial Intelligence Act**) è il primo tentativo a livello globale di **regolamentare in modo orizzontale** tutti i sistemi di intelligenza artificiale, ponendo **l'accento sui rischi** che questi sistemi possano rappresentare per i **diritti fondamentali**, tra cui la **protezione dei dati personali** come definito dall'art. 8 della Carta dei Diritti Fondamentali dell'UE.

A differenza del **GDPR**, che si concentra esclusivamente sul **trattamento dei dati personali**, l'AI Act **non si applica solo quando c'è trattamento di dati personali**. Tuttavia, gran parte dei sistemi IA, come sopra accennato, **necessita di dati personali per funzionare**, quindi, i due regolamenti si sovrappongono frequentemente.

5.2. Come l'AI Act impatta la privacy in dettaglio

5.2.1 Approccio basato sul rischio

L'elemento chiave, come per ormai tutti i sistemi di gestione, è la **classificazione per livelli di rischio**, che determina **quali obblighi si applicano**. I sistemi ad **alto rischio** sono quelli che:

- trattano dati sensibili (biometrici, sanitari, ecc.);
- sono usati in ambiti critici (occupazione, istruzione, giustizia, polizia, infrastrutture);
- possono incidere direttamente sui diritti individuali (es. AI che valuta CV per l'assunzione del personale).

Obblighi specifici che toccano la privacy

a) *Valutazione di conformità*

Chi sviluppa un sistema ad alto rischio dovrà:

- dimostrare che il sistema è **conforme ai requisiti di sicurezza e privacy**;
- mantenere **registri di tracciabilità** (log, documentazione dei dati usati per l'addestramento);
- redigere **valutazioni d'impatto etico e sui diritti fondamentali**, simili alla DPIA del GDPR.

b) *Gestione dei dati*

Per tutelare la privacy e ridurre i rischi di discriminazione si adottano i principi che già sono largamente previsti dal GDPR come di seguito:

- i **set di dati che vengono usati per l'addestramento devono essere di alta qualità**, rappresentativi e privi di *bias*, quindi di ogni forma di pregiudizio;
- devono essere adottati **meccanismi per anonimizzare o pseudonimizzare** i dati;
- è necessario garantire **l'accesso selettivo** ai dati da parte del personale autorizzato.

c) *Trasparenza*

- L'utente finale deve sapere **che sta interagendo con un'AI** (es. chatbot, sistema generativo).
- L'utente deve poter ottenere **spiegazioni comprensibili delle decisioni** prese da AI, specialmente se incidono sui suoi diritti (es. rifiuto di un prestito, esito di un colloquio).
- Devono essere resi disponibili **manuali di istruzione**, interfacce per l'interazione sicura, e strumenti di supervisione umana.

5.2.2 Sistemi vietati

Per proteggere la dignità e i dati delle persone, l'AI Act **proibisce** alcune applicazioni, come:

- sistemi che usano tecniche subliminali per manipolare il comportamento;
- social scoring da parte di enti pubblici;
- riconoscimento biometrico in tempo reale in spazi pubblici (con eccezioni molto ristrette e soggette ad autorizzazioni).

Relazione tra AI Act e GDPR

Aspetto	GDPR	AI Act
Ambito	Tutto il trattamento di dati personali	Tutti i sistemi AI, anche senza dati personali
Focus principale	Privacy, trasparenza, controllo	Rischi sistemici, sicurezza, etica
Principio di responsabilità	Accountability del titolare/trattamento	Responsabilità di provider e deployer
Valutazione d'impatto	DPIA	Risk Assessment + Fundamental Rights Impact
Diritti dell'interessato	Accesso, rettifica, cancellazione, opposizione	Non specifici, ma previsti in parte per quanto riguarda la trasparenza
Supervisione	Autorità privacy nazionali	Autorità di vigilanza IA + coordinamento europeo

I due regolamenti **si rafforzano reciprocamente**, ma richiedono **coordinamento tra i team legali, privacy, sviluppo e sicurezza** nelle aziende e nella PA.

5.2.3 Ruoli e responsabilità

L'AI Act definisce diversi soggetti responsabili:

- **Provider**: chi sviluppa il sistema AI (es. software house);
- **Deployer**: chi lo utilizza (es. azienda che lo integra nei processi HR) o lo mette in uso all'utente finale (es. nel caso di chatbot);
- **Importatore e distributore**: se il sistema arriva da Paesi extra UE.

Ognuno ha **obblighi diversi**, ma chi implementa un sistema AI **non può esimersi dal verificarne la conformità, anche se non è il produttore**.

5.3.2.1 Checklist dettagliata per la conformità all'AI Act in ottica privacy.

Affinché si possa valutare la conformità dei sistemi basati sull'IA, si potrà procedere con l'indagine di quesiti fondamentali, oggetto di apposita check list da utilizzare durante gli audit, relativamente alle seguenti aree:

1. *Identificazione e classificazione del sistema AI*
   - Il sistema utilizza algoritmi di intelligenza artificiale? (machine learning, NLP, visione artificiale, ecc.)
   - Il sistema **tratta dati personali** o biometrici?

- Il sistema rientra in una delle categorie ad **alto rischio** previste dall'AI Act?
  - Reclutamento/HR
  - Giustizia
  - Sorveglianza biometrica
  - Istruzione, esami
  - Finanza e credito
- È stata fatta una **classificazione del rischio AI Act**?

2. *Verifica del trattamento dei dati (conformità GDPR)*
   - È stato individuato il **titolare del trattamento** e i responsabili del trattamento?
   - I dati personali trattati hanno una **base giuridica valida** (es. consenso, obbligo legale)?
   - I dati sono **minimizzati, pertinenti e limitati** allo scopo?
   - Sono adottate tecniche di **anonimizzazione o pseudonimizzazione**, se applicabili?
   - È garantito il **diritto alla spiegazione**, se il sistema prende decisioni automatizzate?
   - È presente una **DPIA (valutazione d'impatto GDPR)**?
3. *Obblighi specifici AI Act per sistemi ad alto rischio*
   - È stata redatta una **valutazione del rischio e dell'impatto sui diritti fondamentali**?
   - Sono documentati e tracciati i **dati di addestramento, test e validazione**?
   - I dati sono **accurati, rappresentativi, privi di bias** (o documentati i limiti)?
   - Esiste un sistema di **gestione della qualità del dataset**?
   - È presente una documentazione tecnica completa per l'AI (design, test, prestazioni)?
   - È garantita la **tracciabilità e auditabilità** del processo decisionale?
   - Sono stati implementati **meccanismi di supervisione umana**?
4. *Obblighi di trasparenza e informazione*
   - Gli utenti sono **informati che stanno interagendo con un'AI**?
   - I contenuti generati artificialmente (es. deepfake) sono **etichettati chiaramente**?
   - Sono predisposte **informative chiare e comprensibili** sugli scopi e il funzionamento dell'AI?
   - È previsto un **meccanismo per esercitare i diritti (GDPR)** in relazione all'AI?
5. *Sicurezza e governance del sistema*

- Sono adottate **misure tecniche e organizzative** per proteggere i dati e ridurre i rischi etici?
- Il sistema è soggetto a **revisioni periodiche, test e monitoraggio continuo**?
- Esiste un registro di tutte le **modifiche e aggiornamenti** del modello?
- Sono previste **procedure di gestione incidenti** e data breach anche per l'IA?

6. *Ruoli e responsabilità (AI Act + GDPR)*
   - È chiaro chi è il **provider (sviluppatore)** e chi è il **deployer (utilizzatore)**?
   - È stato fatto un **accordo di responsabilità** tra provider, integratore e titolare del trattamento?
   - È stata effettuata una **valutazione delle terze parti** (es. fornitori di modelli preaddestrati)?
7. *Supervisione e conformità*
   - È stato designato un referente o team per la **compliance AI + privacy**?
   - È previsto un **audit interno** regolare sui sistemi AI?
   - È predisposta una **procedura di notifica alle autorità competenti**, in caso di incidenti?
   - Sono in atto programmi di **formazione continua** per chi gestisce l'AI?
8. *Documenti necessari*
   - DPIA (valutazione d'impatto GDPR)
   - Impact Assessment AI Act (diritti fondamentali)
   - Informative agli interessati (privacy + IA)
   - Registro delle attività AI ad alto rischio
   - Documentazione tecnica del sistema AI
   - Registro dei log, audit e supervisioni
   - Accordi di responsabilità tra provider e utenti

Bibliografia e sitografia

REGISTRO DELLE VIOLAZIONI – "DATA BREACH"

- GDPR regolamento 2016/679 Data Breach – Violazione dati personali. Servizi.gpdp.it/databreach/s/
- Data breach – come fare il registro delle violazioni. Federprivacy.org
- Registro data breach. Vademecum per le aziende. Agendadigitale.eu

REGISTRO DELL'AMMINISTRATORE DI SISTEMA

- Amministratore di sistema. Compiti e responsabilità del ruolo. *Archimedia.it*; *protezionedatipersonali.it*
- Amministratore di sistema GDPR. Unolegal.it
- Amministratori di sistema: ruolo, responsabilità e rischi ai tempi del GDPR. Osservatori.net
- L'amministratore di sistema e la privacy. Ordine dei Dottori Commercialisti ed Esperti Contabili di Brescia – Scheda tecnica n. 2/10

REGISTRO DEI TRATTAMENTI DEI DATI PERSONALI

- Misure e accorgimenti prescritti di titolare dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema. *G.U. n. 300 del 24 dicembre 2008* Registro delle attività di trattamento. *garanteprivacy.it*
- La bussola della privacy – Registro delle attività di trattamento. Magazine.gdprscuola.it

REGISTRO DEI VISITATORI E PROTEZIONE DELLA PRIVACY

- Registro dei visitatori e protezione della privacy. Dirittodellinformazione.it
- Registro dei visitatori: un trattamento ai dati personali poco considerato. Saef.it

REGISTRO DELLA FORMAZIONE

- Formazione privacy obbligatoria col GDPR. Agendadigitale.eu
- Formazione privacy: un obbligo di legge previsto dal GDPR. Rsm.global
- L'obbligo di formazione previsto dal GDPR. Gdprprivacy.eu

NIS 2

- Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3°32022L2555
- Agenzia per la Cybersicurezza Nazionale (ACN) – Italia https://www.acn.gov.it
- ENISA – Agenzia dell'Unione Europea per la Cybersecurity https://www.enisa.europa.eu/

ARTIFICIAL INTELLIGENCE ACT

- Artificial Intelligence Act (Proposta di Regolamento Europeo sull'IA) https://artificialintelligenceact.eu/https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206
- Regolamento Generale sulla Protezione dei Dati (GDPR – UE 2016/679) https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679
- Carta dei Diritti Fondamentali dell'Unione Europea (Articolo 8 – Protezione dei dati personali) https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A12012P%2FTXT
- European Data Protection Board (EDPB) – Linee guida su IA e privacy https://edpb.europa.eu/
- Commissione Europea – Strategia sull'Intelligenza Artificiale https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
- European AI Office (futuro organismo europeo di supervisione sull'IA)
- https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-artificial-intelligence-office_en

ANALISI DEI RISCHI E DPIA

- https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-
- https://enisa.europa.eu/
- https://www.aepd.es/
- https://cnil.fr/fr

Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili
Piazza della Repubblica, 59 00185 Roma