Luca Di Leo

Consulenza e formazione in materia di protezione dei dati personali dal 2005

Studio Paci &C srl
(cda)

Associazione Protezione diritti e libertà privacy
(Vice presidente)

Associazione Protezione Diritti e Libertà Privacy

Contatti:
dileo@sistemcom.it
Cell. 3931019939

Linkedin: #luca di leo

Responsabile della Protezione dei Dati (DPO per aziende private, pubbliche, sanità)
certificazione UNI 11697:2017 (Registro Accredia)

Valutatore Privacy
certificazione UNI 11697:2017 (Registro Accredia)

Privacy Officer
Certificazione TUV Italia 2013 – certificazione competenze Federprivacy – Legge n.4/2013

Auditor GDPR
secondo lo schema di certificazione per il GDPR: ISDP@10003 (Registro AICQ SICEV)

Consulente per l'implementazione dello schema di certificazione ISDP@10003
(Ente di certificazione INVEO)

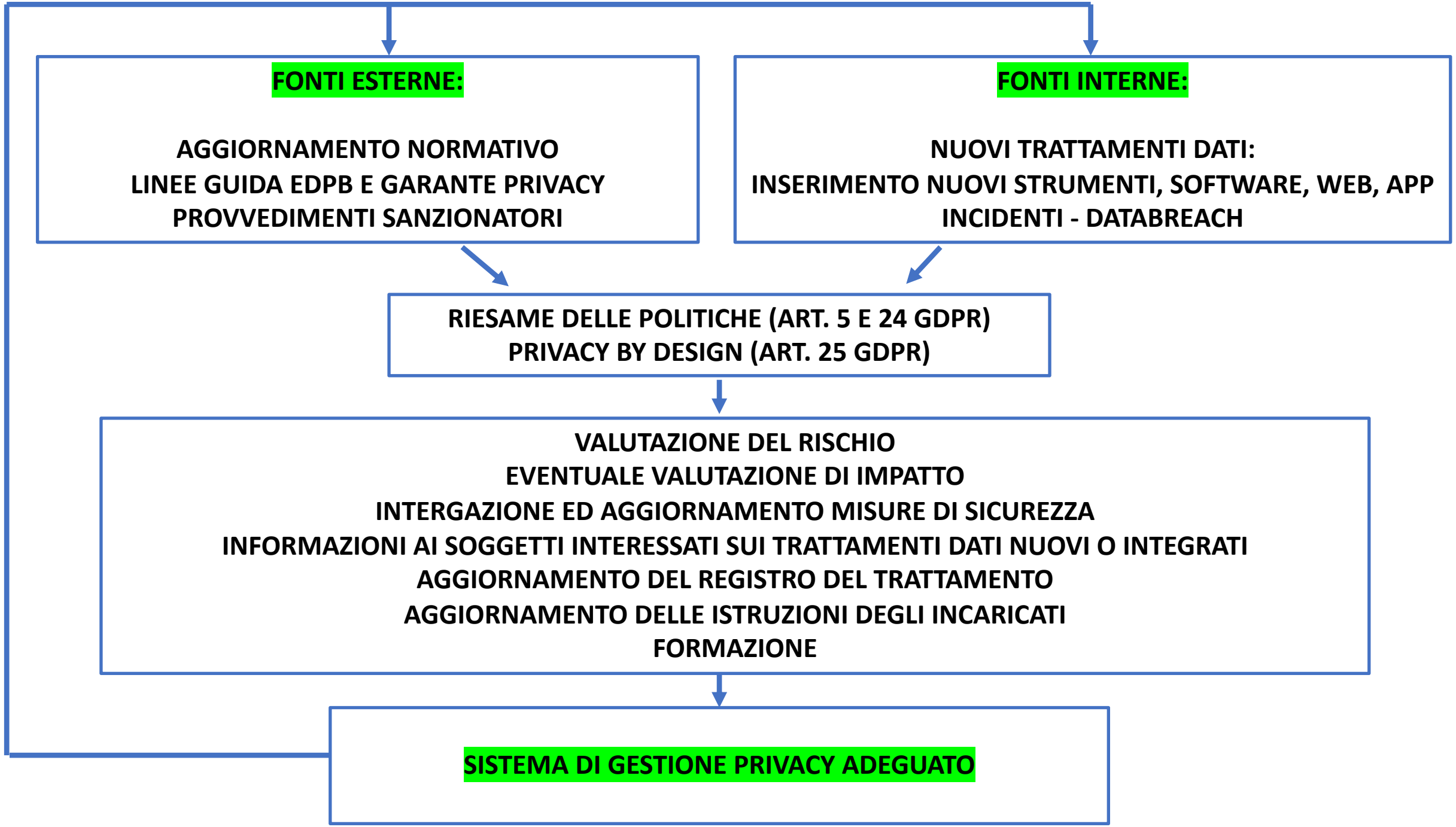
Lead Auditor ISO 27001 , aggiornamento ISO 27701

VARIABILI ESTERNE:

DECRETO TRASPARENZE
WHISTLEBLOWING
CONTROLLO DEL LAVORATORE – LOG FILE – INTERNET – POSTA ELETTRONICA
CYBERSECURITY

VARIABILI INTERNE:

MODIFICHE ED INTEGRAZIONI DEI TRATTAMENTI DATI ALL'INTERNO DELL'ORGANIZZAZIONE


FONTI ESTERNE:
AGGIORNAMENTO NORMATIVO
LINEE GUIDA EDPB E GARANTE PRIVACY
PROVVEDIMENTI SANZIONATORI
FONTI INTERNE:
NUOVI TRATTAMENTI DATI:
INSERIMENTO NUOVI STRUMENTI, SOFTWARE, WEB, APP
INCIDENTI - DATABREACH
RIESAME DELLE POLITICHE (ART. 5 E 24 GDPR)
PRIVACY BY DESIGN (ART. 25 GDPR)
VALUTAZIONE DEL RISCHIO
EVENTUALE VALUTAZIONE DI IMPATTO
INTERGAZIONE ED AGGIORNAMENTO MISURE DI SICUREZZA
INFORMAZIONI AI SOGGETTI INTERESSATI SUI TRATTAMENTI DATI NUOVI O INTEGRATI
AGGIORNAMENTO DEL REGISTRO DEL TRATTAMENTO
AGGIORNAMENTO DELLE ISTRUZIONI DEGLI INCARICATI
FORMAZIONE
SISTEMA DI GESTIONE PRIVACY ADEGUATO

Garante per la protezione dei dati:
Parere su uno schema di decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (cd. direttiva whistleblowing) - 11 gennaio 2023

"Whistleblowing"

relatore: Luca Di Leo

Studio Paci &C srl

Whistleblowing e GDPR

Con il termine whistleblowing s'intende:

la rivelazione spontanea da parte di un individuo, detto "segnalante" (in inglese "whistleblower") di un illecito o di un'irregolarità commessa all'interno dell'organizzazione, del quale lo stesso sia stato testimone nell'esercizio delle proprie funzioni.
Il segnalante spesso è un dipendente ma può anche essere una terza parte, per esempio un fornitore o un cliente.

Si parla di whistleblowing "interno" quando la segnalazione viene fatta da un dipendente dell'azienda per il tramite di canali di segnalazione interni all'azienda.

Questi strumenti hanno allo scopo di garantire una canale di comunicazione a tutti coloro che sono a conoscenza di illeciti o atti non etici avvenuti all'interno dell'organizzazione.

Ed è proprio qui che la disciplina sulla protezione dei dati personali trova applicazione!

Di fatto il Reg. UE 2016/679 «GDPR» si applica a tutti i trattamenti dati dell'organizzazione, ed in particolare in questo contesto occorre disciplinare i canali di comunicazione in termini di sicurezza, e:

Whistleblowing e GDPR

Da fare:

- aggiornare il registro del trattamento,

- la valutazione dei rischi,

- potrebbe essere necessaria una valutazione di impatto se si utilizzano nuove tecnologie in quanto possono introdurre rischi non valutati precedentemente.

- misure di sicurezza applicate al canale di comunicazione ed al trattamento stesso.

- nonché redigere una informativa specifica ai lavoratori, ed istruzioni per il trattamento ai soggetti reputati a ricevere tali segnalazioni.

- Se ci si avvale di servizi esterni per l'utilizzo dei canali di segnalazione occorre anche valutare in termini di garanzie di applicazione al GDPR del soggetto ed individuarlo quale responsabile del trattamento, e quindi occorrerà la formulazione di una nomina a responsabile da fare sottoscrivere a tale soggetto..

Le aziende si possono avvalere sia della posta elettronica, che

di servizi web o APP che alcuni fornitori di servizi rivendono.

Whistleblowing e GDPR

Tali disposizioni prescrivono le condizioni per l'attivazione e la gestione,

nel settore pubblico e in

quello privato

di canali che consentano l'effettuazione di segnalazioni con obbligo di:

- Garanzia (anche mediante il ricorso alla crittografia) della riservatezza del segnalante,

- delle persone coinvolte e menzionate nella segnalazione,

- nonché del contenuto della stessa.

I canali di segnalazione interna assurgono, peraltro, ad oggetto necessario dei modelli di organizzazione e gestione di cui all'articolo 6, c.1, lett. a) del d.lgs. 231 del 2001.

D.Lgs. 104 del 27/6/2022 «Decreto trasparenza»
in attuazione della direttiva direttiva (UE) 2019/1152

"Aspetti riguardanti la normativa sulla protezione dei dati personali nel decreto trasparenza"

a seguito delle Questioni interpretative e applicative in materia di protezione dei dati del 24 gennaio 2023 del Garante per la Protezione dei dati

relatore: Luca Di Leo

Studio Paci &C srl

Questioni interpretative e applicative sul «Decreto Trasparenza»

interpretazioni del Garante del 24 gennaio 2023 riguardanti il decreto trasparenza di agosto 2022,

la normativa prevede che il datore di lavoro in qualità di titolare del trattamento debba informare i lavoratori della presenza di:

sistemi di monitoraggio che in qualche modo possano contribuire a decisioni riguardanti il rapporto di lavoro dei dipendenti.

In tale interpretazione del decreto il Garante ricorda quali siano gli adempimenti che le aziende devono porre in essere e quali accortezze occorre avere.

Questioni interpretative e applicative sul «Decreto Trasparenza»

“sistemi decisionali o di monitoraggio automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori”.

Questioni interpretative e applicative sul «Decreto Trasparenza»

strumenti e tecnologie, quali:
"software per il riconoscimento emotivo",
"strumenti di data analytics o machine learning, rete neurali, deep-learning", nonché
"sistemi per il riconoscimento facciale, sistemi di rating e ranking",

che, specie se impiegati nel contesto lavorativo, determinano un elevato livello di rischio per i diritti e le libertà degli interessati oggetto di specifica tutela nell'ambito del sistema di protezione dei dati personali.

L'impiego di tali sistemi di monitoraggio particolarmente invasivi, pone, anzitutto, un tema di liceità dei trattamenti di dati personali effettuati mediante gli stessi, tenuto conto della disciplina di settore in materia di impiego di strumenti tecnologici nel contesto lavorativo (v. art. 114 del Codice, che rimanda all'art. 4 della L. 300/1970).

Le specificità delle tecnologie di questi sistemi, nonché la natura dei dati trattati (ad esempio, **i dati biometrici e quelli relativi alle emozioni del lavoratore**) e le funzionalità che spesso ad essi sono associate, **sollevano, altresì, dubbi in ordine alla stessa proporzionalità del loro impiego, nonché di compatibilità con i principi generali in materia di protezione dei dati e con il quadro di garanzie in materia di libertà e dignità del lavoratore**, potendosi, peraltro, porsi in contrasto con le disposizioni nazionali che vietano al datore di lavoro di trattare informazioni attinenti alla sfera privata del lavoratore (v. art. 113 del Codice, che rimanda all'art. 8 della L. 300/1970).

Questioni interpretative e applicative sul «Decreto Trasparenza»

Tra le informazioni ulteriori **che il datore di lavoro, in qualità di titolare del trattamento, deve fornire all'interessato rientrano:**

- gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi decisionali o di monitoraggio automatizzati; - il funzionamento dei sistemi;
- i parametri principali utilizzati per programmare o addestrare i sistemi decisionali o di monitoraggio automatizzati, inclusi i meccanismi di valutazione delle prestazioni;
- le misure di controllo adottate per le decisioni automatizzate,
- gli eventuali processi di correzione e il responsabile del sistema di gestione della qualità;
- il livello di accuratezza, robustezza e cibersicurezza dei sistemi decisionali o di monitoraggio automatizzati e le metriche utilizzate per misurare tali parametri, nonché
- gli impatti potenzialmente discriminatori delle metriche stesse.

Tra gli elementi che, invece, specificano la portata di quanto già compreso negli artt. 13 e 14 del Regolamento, rientrano:

✓ la logica dei sistemi decisionali o di monitoraggio automatizzati, la cui indicazione, nell'impianto degli artt. 13 e 14, è espressamente richiesta nel caso di ricorso ai processi decisionali automatizzati, compresa la profilazione, di cui all'art. 22 del Regolamento;
✓ l'indicazione delle categorie di dati trattati,

Questioni interpretative e applicative sul «Decreto Trasparenza»

Log di accesso agli strumenti ed applicazioni informatici (es. registrazione degli accessi quali log in, log out, data e ora, nome utente)

Log di navigazione internet (registrazione temporanea della navigazione internet di tutti gli utenti della rete informatica per finalità di sicurezza)

Sistemi di antivirus, prevenzione di virus, malware, phishing, criptlocker, etc. che monitorano automaticamente le attività svolte (sonde / SOK / agent) dagli utenti dei dispositivi elettronici (computer, server, notebook, smartphone, etc.) per finalità di sicurezza

Sistemi hardware o software che possono influire nelle decisioni sui seguenti aspetti:

- decisioni sulle assunzioni di dipendenti (ad esempio chatbot, assistenti virtuali, sistemi automatici di selezione, selezione mediante test o questionari informatici, etc.)
- automatismi per il conferimento degli incarichi ai dipendenti
- automatismi per la verifica del rendimento del lavoratore, delle attività svolte, report sull'efficienza delle lavorazioni o delle prestazioni dei servizi, tempi di esecuzione delle consegne, o dei lavori
- sistemi automatici o semi-automatici che concorrono a stabilire il termine / cessazione del rapporto di lavoro, attraverso un monitoraggio
Sistema di videosorveglianza che monitora per finalità di sicurezza del lavoro l'esecuzione di lavorazioni particolari
Sistema di geolocalizzazione che monitora tempi e percorsi (al fine di rendere indicazioni per ottimizzare gli stessi, stabilire a quali clienti consegnare la merce, su quali posti recarsi per svolgere l'attività lavorativa, etc)

Questioni interpretative e applicative sul «Decreto Trasparenza»

- a) gli aspetti del rapporto di lavoro sui quali incide l'utilizzo dei sistemi di cui al comma 1;
  (elenco degli strumenti censiti nella valutazione del rischio o DPIA - registro del trattamento)

- b) gli scopi e le finalita' dei sistemi di cui al comma 1;
  (informativa e registro del trattamento)

- c) la logica ed il funzionamento dei sistemi di cui al comma 1;
  (Informativa, registro del trattamento)

- d) le categorie di dati e i parametri principali utilizzati per programmare o addestrare i sistemi di cui al comma 1, inclusi i meccanismi di valutazione delle prestazioni; (**descrizione specifica**, registro del trattamento, valutazione di impatto, regolamento / disciplinare aziendale)

- e) le misure di controllo adottate per le decisioni automatizzate, gli eventuali processi di correzione e il responsabile del sistema di gestione della qualita'; (misure di sicurezza derivanti dalla valutazione del rischio / di impatto, registro del trattamento)

- f) il livello di accuratezza, robustezza e cibersicurezza dei sistemi di cui al comma 1 e le metriche utilizzate per misurare tali parametri, nonche' gli impatti potenzialmente discriminatori delle metriche stesse. (misure di sicurezza derivanti dalla valutazione del rischio / di impatto, simulazioni di penetration test)

VERIFICARE NECESSITA' DI ACCORDO SINDACALE O RICH. AUTORIZZAZIONE DA PARTE DELL'ISPETTORATO DEL LAVORO

Aspetti sul controllo del lavoratore derivante dai trattamenti dati relativi alla registrazione dei

«file log»
«backup metadati posta elettronica»
«log navigazione internet»

a seguito di alcuni provvedimenti sanzionatori del Garante per la Protezione dei dati

Chiederemo di integrare alcune informazioni rispetto ai sistemi informatici

Penetration test sulla sicurezza dell'infrastruttura informatica

Abbiamo registrato diversi incidenti e databreach
occorsi sia a società private che a pubbliche amministrazioni,

è giunta l'ora di effettuare penetration test sulla sicurezza dell'infrastruttura informatica

al fine di scongiurare hackeraggi, eventi malevoli, phishing,

ma anche al fine di essere compliance al regolamento per la privacy by default,

e le misure di sicurezza di cui all'art. 32 che prevedono la verifica costante dell'efficacia delle misure di sicurezza implementate.

PER QUESTO A SEGUIRE UNA SESSIONE FORMATIVA DI AGGIORNAMENTO SULLE MISURE DI SICUREZZA E SULLA CIBERSICUREZZA, CHE OGNUNO DI NOI PUO' METTERE IN ATTO PER NON COMPROMETTERE LA SICUREZZA DELL'INFRASTRUTTURA INFORMATICA AZIENDALE.