NUOVI PERCORSI DI SVILUPPO
DELLA CAPACITÀ AMMINISTRATIVA
DELLA REGIONE SICILIANA

5 maggio 2021

Avv. Ernesto Belisario

IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO E L'ADEGUATEZZA DELLE MISURE DI SICUREZZA

Unione Europea
Repubblica Italiana
Regione Siciliana
FSE FONDO SOCIALE EUROPEO
SICILIA 2020
PROGRAMMA OPERATIVO
FormezPA

Sommario


General Data
Protection Regulation

I – I SOGGETTI COINVOLTI NEL TRATTAMENTI: RUOLI E RESPONSABILITÀ

CODICE PRIVACY

1.Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

2.Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

(Art. 2-quaterdecies, D. Lgs. n. 196/2003)

GDPR


TITOLARE DEL TRATTAMENTO
RESPONSABILE DEL TRATTAMENTO (esterno)
RESPONSABILE DELLA PROTEZIONE DEI DATI
AUTORIZZATI AL TRATTAMENTO
SUB-RESPONSABILE

TITOLARE DEL TRATTAMENTO

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Art. 4, par. 1, GDPR

FUNZIONI E COMPITI

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

(Art. 2-quaterdecies, D. Lgs. n. 196/2003)

AUTORIZZATI, INCARICATI E DESIGNATI

Pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex art. 30 Codice Privacy), il Regolamento non ne esclude la presenza in quanto fa riferimento a «persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile».

RESPONSABILE DEL TRATTAMENTO

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Art. 4, par. 1, GDPR

RESPONSABILE DEL TRATTAMENTO

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

Art. 28, par. 1, GDPR

RESPONSABILE DEL TRATTAMENTO

- ✓ *trattare i dati personali soltanto su istruzione documentata del titolare del trattamento;*
- ✓ *garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;*
- ✓ *adottare le misure di sicurezza;*
- ✓ *rispettare i limiti previsti per la nomina dei sub-responsabili;*
- ✓ *assistere il titolare del trattamento in relazione all'esercizio dei diritti degli interessati;*
- ✓ *cancellare o restituire al titolare tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti;*
- ✓ *mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.*

Art. 28, par. 3, GDPR

RESPONSABILE DEL TRATTAMENTO

ATTENZIONE ALLA NOMINA

Il Garante italiano ha sanzionato un'azienda ospedaliera per € 80,000.00 per il trattamento illecito di dati di oltre 2000 aspiranti infermieri. L'azienda ospedaliera ha affidato alla società fornitrice della piattaforma la fase di raccolta e preselezione delle candidature senza però opportunamente regolare il rapporto ai sensi dell'art. 28 GDPR.

La sanzione è stata comminata anche a causa di una erronea individuazione della base giuridica che per il trattamento di dati, ivi inclusi quelli particolari, volti all'assunzione di personale da parte di un soggetto pubblico, che non coincide con il consenso bensì con l'adempimento di un obbligo di legge o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare stesso.

ATTENZIONE ALLA NOMINA

Il Garante italiano ha sanzionato una pubblica amministrazione per € 500.000,00 per molteplici condotte scorrette tra cui la mancata nomina del fornitore ai sensi dell'art. 28 GDPR per le attività di assistenza e manutenzione.

L'Autorità polacca ha sanzionato per € 9.380,00 un ente pubblico per nominato il fornitore cui era affidato in outsourcing il servizio di bollettino comunale.

RESPONSABILE PROTEZIONE DATI

QUANDO È OBBLIGATORIO IL DPO

La designazione del DPO è obbligatoria (da parte del Titolare o del Responsabile del trattamento) solo se:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'art. 9 o 10 GDPR.

COMPITI DEL DPO

- Informare e fornire al Titolare, al Responsabile nonché ai dipendenti che eseguono il trattamento, consulenza in merito agli obblighi normativi in materia;
- Sorvegliare l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche in materia del Titolare o del Responsabile del trattamento, compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale che partecipa al trattamento e al controllo in merito;
- Fornire, se richiesto, pareri sulla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- Cooperare con l'Autorità di controllo e fungere da punto di contatto con il Garante per la protezione dei dati di personali per questioni connesse al trattamento.

IL RUOLO DEL DPO

- Il DPO va designato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i propri compiti.
- È figura apicale, assolutamente diversa quanto a ruolo e funzioni dal "semplice" responsabile del trattamento.
- Può essere un dipendente del Titolare o del Responsabile del trattamento oppure un consulente esterno che assolve i suoi compiti in base a un contratto di servizi.
- I dati di contatto del DPO vanno comunicati al Garante per la protezione dei dati personali e resi pubblici.

IL RUOLO DEL DPO

Il DPO deve essere autonomo ed indipendente:

non deve ricevere dal Titolare o dal Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati né è soggetto a potere disciplinare o sanzionatorio per l'adempimento dei propri compiti.

deve avere le risorse necessarie e il potere di spesa per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere le proprie conoscenze specialistiche (es. aggiornamento professionale).

IL DPO E GLI INTERESSATI

Il RPD, se necessario con il supporto di un team di collaboratori, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa.
Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

(Linee Guida Gruppo Art. 29)

RESPONSABILITÀ DEL DPO

I DPO non rispondono personalmente in caso di inosservanza del GDPR. Quest'ultimo chiarisce che spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, primo paragrafo). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare o sul responsabile.

(Linee Guida Gruppo Art. 29)

GESTIONE IN FORMA ASSOCIATA

Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

(Art. 37, par. 3, GDPR)

DPO INTERNO

- *Nel caso in cui si opti per un RPD interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.*
- *È necessario apposito atto di designazione*

DPO ESTERNO

- Nel caso dei DPO esterno, le funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica. Se la funzione di DPO è svolta da un fornitore esterno di servizi, i compiti stabiliti per il DPO potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale DPO soddisfi tutti i requisiti applicabili come fissati nel GDPR.
- Necessario fare attenzione alla procedura di evidenza per la scelta del DPO (valore affidamento, requisiti partecipanti, SLA contratto)

AUTORITÀ DI CONTROLLO

Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»).

(Art. 51, par. 1, GDPR)

AUTORITÀ DI CONTROLLO

L'Autorità di controllo di cui all'articolo 51 del Regolamento è individuata nel Garante per la protezione dei dati personali.

(Art. 2-bis, comma 1, D. Lgs. n. 196/2003)

COMPITI DEL GARANTE

- ✓ *esercitare i poteri previsti dal GDPR per le Autorità di controllo controllare se i trattamenti sono effettuati nel rispetto della*
- ✓ *disciplina applicabile, anche in caso di loro cessazione trattare i reclami*
- ✓ *promuovere l'adozione di regole deontologiche*
- ✓ *denunciare i fatti configurabili come reati perseguibili d'ufficio trasmettere la relazione annuale al Parlamento e al Governo assicurare la tutela dei diritti e delle libertà fondamentali*

ACCERTAMENTI

Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

(Art. 158, comma 1, D. Lgs. n. 196/2003)

AUTORIZZAZIONI

Il Garante per la protezione dei dati personali, con provvedimento di carattere generale da porre in consultazione pubblica entro novanta giorni dalla data di entrata in vigore del presente decreto, individua le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché al Capo IX del regolamento (UE) 2016/679, che risultano compatibili con le disposizioni del medesimo regolamento e del presente decreto e, ove occorra, provvede al loro aggiornamento. Il provvedimento di cui al presente comma è adottato entro sessanta giorni dall'esito del procedimento di consultazione pubblica.

(Art. 21, comma 1, D. Lgs. n. 196/2003)

PROVVEDIMENTI GENERALI

A decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto.

(Art. 22, comma 4, D. Lgs. n. 101/2018)

II – IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO COME NUOVO ADEMPIMENTO DEL GDPR

REGISTRO DEL TRATTAMENTO

Ogni titolare del trattamento tiene un registro elettronico in cui sono riportate le seguenti informazioni:

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

b)le finalità del trattamento;

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

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

e)ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;

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

g)ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

(Art. 30, par. 1, GDPR)

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

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

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

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

Modello rilevazione dati per Titolare dei trattamenti effettuati ai sensi del Regolamento UE 679/2016 (GDPR)

Cognome e nome del Titolare			
Nella qualità di			
Email Titolare		PEC	
Indirizzo		Tel	

Informazioni art. 30 del GDPR									Informazioni particolari							
N	Denominazione del trattamento	Finalità del trattamento	Categorie dei soggetti interessati (a cui si riferiscono i dati)	Categorie dei dati personali trattati	Categorie di destinatari a cui i dati sono o possono essere comunicati	Eventuali paesi terzi o organizzazioni internazionali alle quali i dati possono essere comunicati i dati	Indicazione garanzie adottate per il trasferimento internazionale (se applicabile)	Eventuali Termini previsti per la cancellazione	Responsabile del Trattamento	Nella qualità di	E' stato emesso il Decreto del Titolare di nomina del Responsabile?	Altri sub-Responsabili esterni (che intervengono parzialmente sul trattamento dati)	Art. 6 del GDPR (base giuridica su cui si fonda il trattamento)	Art. 9 del GDPR (base giuridica per il trattamento di particolari categorie di dati)	Categoria di trattamento	Come vengono conservati i dati

Esempi di dati da riportare nel modello di rilevazione

Titolare	Responsabile	Finalità	Categorie di Interessati	Categorie di dati	Categorie di destinatari	Garanzie trasferimento estero	Esempi misure di sicurezza	Base giuridica del trattamento	Base giuridica ex art. 9	Modalità conservazione dati	Categoria di trattamenti	Consenso	Fase DPIA	SI/NO
Presidente della Regione	Dirigente Generale (specificare)	Amministrazione del personale	Dipendenti	Dati personali di identificazione	L'Interessato	Decisione di adeguatezza	**1) - Misure organizzative:**	Consenso dell'interessato	Consenso dell'interessato	Digitale presso l'Amministrazione	Raccolta	Comportamentale	Da valutare	SI
Assessore regionale (specificare)	Dirigente Area / Servizio (specificare)	Gestione del personale	Utenti	Dati di identificazione elettronica	Coloro che hanno rapporti con l'Interessato	Consenso dell'Interessato	1 a. nomina per iscritto personale	Esecuzione di un contratto	Esercizio obblighi in materia di diritto del lavoro	Digitale presso società in house	Registrazione	Espresso	Da avviare	NO
	Dirigente UO (specificare)	Gestione di assicurazione sanitaria	Fornitori	Dati di identificazione biometrica	Consulenti professionisti dell'Interessato	Regole amministrative vincolanti	1 b. istruzioni per il trattamento	Esecuzione misure precontrattuali	Esercizio obblighi in materia di protezione sociale	Digitale presso società esterna	Organizzazione	Per iscritto	In corso	
	Dirigente posizione di collaborazione (specificare)	Assicurazione incidenti sul lavoro	Pazienti	Dati sulla salute fisica	Datore di lavoro	Clausole standard	1 c. accesso controllato	Obbligo legale	Esercizio obblighi in materia di protezione sociale	Digitale in Cloud	Strutturazione	Documentato	Conclusa	
	Capo di Gabinetto (specificare)	Gestione l. 81/2008	Cittadini	Dati di identificazione finanziaria	Amministrazioni pubbliche	Trasferimento su deroga per situazioni specifiche	1 d. armadi chiusi	Salvaguardia interessi vitali dell'interessato	Tutela interesse vitale dell'Interessato	Cartacea	Conservazione	Altro	Sospesa (specificare i motivi)	

IL REGISTRO DEL RESPONSABILE

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

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

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

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

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

(Art. 30, par. 2 GDPR)

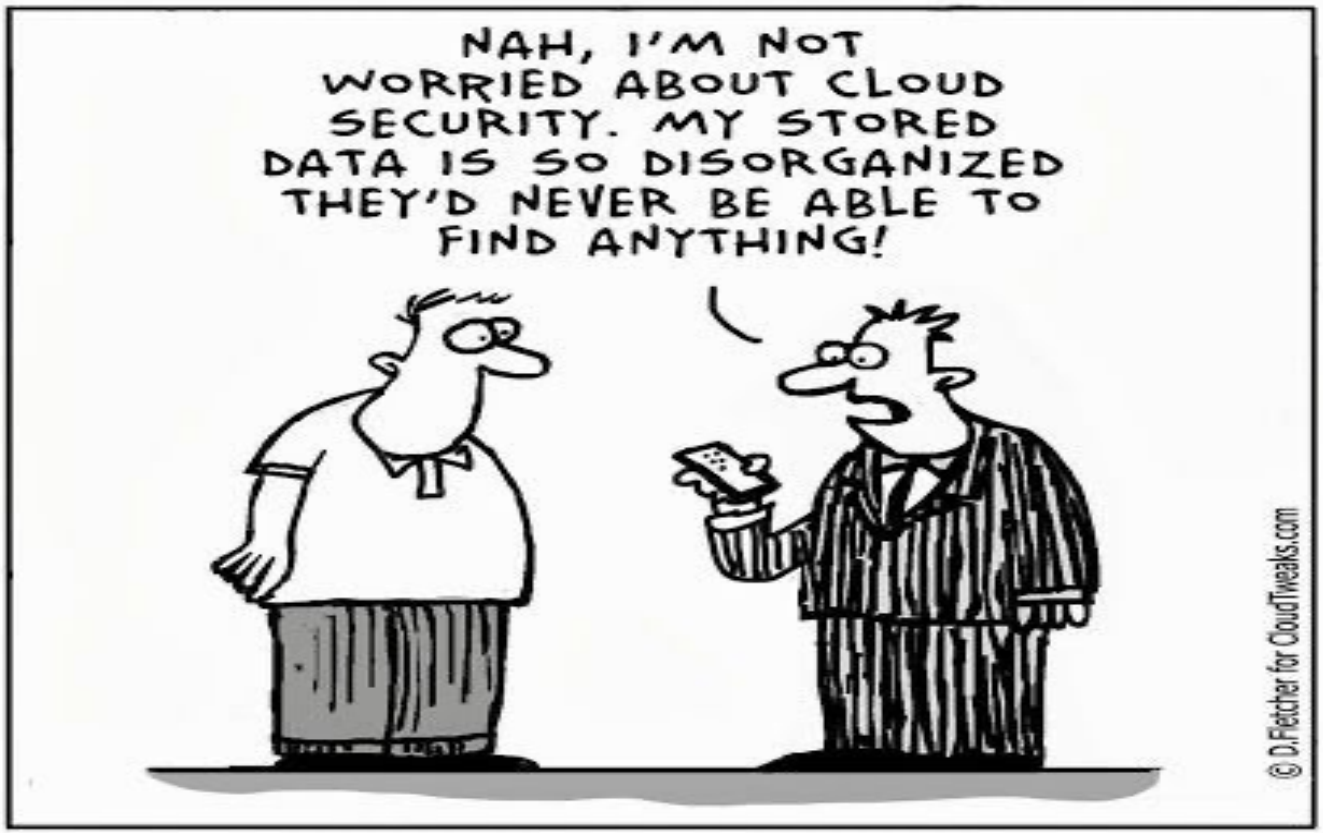
CONSERVAZIONE E AGGIORNAMENTO DEL REGISTRO

Il registro deve essere mantenuto costantemente aggiornato per rispecchiare in maniera effettiva i trattamenti posti in essere dal titolare o dal responsabile.

Qualsiasi cambiamento riferito alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il registro può essere cartaceo o elettronico, e deve recare la data di creazione e successivamente, le date degli aggiornamenti effettuati.

III – L'ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE DAL TITOLARE


NAH, I'M NOT WORRIED ABOUT CLOUD SECURITY. MY STORED DATA IS SO DISORGANIZED THEY'D NEVER BE ABLE TO FIND ANYTHING!
© D.Fletcher for CloudTweaks.com

ADEMPIMENTI PER LA SICUREZZA

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a)la pseudonimizzazione e la cifratura dei dati personali;

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

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

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

(Art. 32, par. 1, GDPR)

MISURE DI SICUREZZA

- Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

- Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento.

Misure Tecniche

La misura tecnica è affidata ad uno strumento, ad una macchina o ad un elaboratore. La conformità in questo caso, dipende dalla correttezza della programmazione della macchina e della sua funzionalità.

Esempi di misure tecniche:

Pseudonimizzazione (Encryption; Masking; Tokenizzazione)

Misure Organizzative

La misura organizzativa è affidata ai comportamenti delle persone, conformi ad uno standard operativo codificato in regole aziendali/protocolli operativi.

Esempi di misure organizzative:

- Controlli degli accessi
- Controlli dei supporti cartacei
- Protezione ambienti e risorse di rete
- Gestione della password

PSUDONIMIZZAZIONE

il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

(Art. 4 GDPR)

LA VALUTAZIONE DELLA COMPLIANCE

Al fine di monitorare dall'interno il rispetto delle policy in materia di protezione dei dati personali viene adottato, sulla base del modello proposto dal RPD aggiornabile all'occorrenza, un questionario di autovalutazione, da compilarsi semestralmente a cura di ciascun dipartimento o ufficio equiparato.

Il questionario consente di monitorare il grado di aderenza dell'attività amministrativa alla norma comunitaria, misurando periodicamente gli sviluppi e rilevando le criticità, al fine di porre in essere interventi correttivi.

Alla compilazione del questionario provvede ogni Responsabile preposto a struttura di massima dimensione, Ufficio di diretta collaborazione, Ufficio alle dirette dipendente o Ufficio Speciale, con il supporto del Referente Privacy, il quale avrà cura di tenere conto adeguatamente dei trattamenti dei dati personali effettuati negli uffici periferici dell'Amministrazione.

Il Dipartimento della Funzione Pubblica e del Personale, ricevuti i questionari, provvederà alla redazione di un report annuale da sottoporre alla Giunta regionale, nel quale siano definiti, di concerto con il RPD, i principali interventi correttivi.

SANZIONE PER CARENTI MISURE DI SICUREZZA

L'Autorità italiana ha sanzionato per € 60,000.00 una società che gestiva la piattaforma dedicata alla raccolta delle domande online di aspiranti infermieri a un concorso pubblico.

I profili contestati hanno riguardato:

-utilizzo del protocollo di trasmissione «http»;

-conservazione dei dati sulla piattaforma anche successivamente alla scadenza del contratto;

-la trasmissione dei dati raccolti sulla piattaforma al titolare tramite CD-ROM privo di qualsivoglia misura di sicurezza. In questo modo, i dati erano liberamente accessibili a chiunque fosse venuto il possesso del supporto di memorizzazione.

Provvedimento n. 161 del 17/09/2020

SANZIONE PER CARENTI MISURE DI SICUREZZA

L'Autorità slovacca sanziona una società per aver cestinato dei documenti nella spazzatura pubblica non sminuzzati.

ICO sanziona per 320,000.00 € un'azienda operante in ambito farmaceutico per aver immagazzinato cinquecentomila documenti contenenti dati comuni e sanitari in contenitori non chiusi e lasciati nel retro di uno stabile; la società non ha protetto accuratamente i dati neppure dagli eventi atmosferici e l'acqua li ha distrutti.

PERMESSI DI AUTORIZZAZIONE

L'Autorità italiana ha sanzionato per 30.000,00 un'Azienda ospedaliera per aver reso accessibili dati sanitari di alcuni pazienti a soggetti non autorizzati. Ciò ha determinato la possibilità di accesso, da parte di specializzandi e di un radiologo, alle cartelle cliniche dei colleghi. In definitiva le misure tecniche di protezione sono risultate inadeguate.

L'autorità per la protezione dei dati portoghese ha sanzionato per € 400.000,00 un ospedale perché pur avendo solo 296 dottori, quasi 900 persone potevano accedere e modificare i fascicoli sanitari dei pazienti.

IV – IL RISPETTO DEI PRINCIPI DI PRIVACY BY DESIGN E PRIVACY BY DEFAULT

PRIVACY BY DESIGN

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Art. 25, par. 1 GDPR

PRIVACY BY DESIGN..IN PRATICA

Il Garante italiano ha sanzionato un partito politico per il mancato e completo tracciamento degli accessi al database di una piattaforma elettorale online e delle operazioni compiute sulla stessa. La sanzione di € 50.000,00 ha riguardato anche la condivisione delle credenziali di autenticazione da parte di più incaricati dotati di elevati privilegi per la gestione della piattaforma e la mancata definizione e configurazione dei differenti profili di autorizzazione in modo da limitare l'accesso ai soli dati necessari nei diversi ambiti di operatività.

PRIVACY BY DESIGN..IN PRATICA

L'Autorità Garante ha sanzionato un'Università italiana per € 30.000,00 per aver reso disponibili online le identità di due *whistleblower* a causa di inadeguate misure di sicurezza e controllo della gestione del sistema di *whistleblowing*, che non sono state in grado di limitare l'accesso a tali dati ai soli soggetti autorizzati.

«*In particolare nel corso dell'istruttoria è emerso che l'accesso all'applicativo whistleblowing avveniva mediante l'indirizzo web* [..]".

Il protocollo di rete utilizzato "http" (hypertext transfer protocol) utilizzato per il trasporto dei dati non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato. Il mancato utilizzo di strumenti di crittografia per il trasporto dei dati si pone quindi in contrasto con l'art. 32 del Regolamento, che peraltro al par. 1, lett. a), individua espressamente la cifratura dei dati come una delle possibili misure di sicurezza idonea a garantire un livello di sicurezza adeguato al rischio».

PRIVACY BY DEFAULT

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Art. 25, par. 2 GDPR

V – VIOLAZIONI DI DATI PERSONALI

Violazioni di dati personali (Data Breach)

DATA BREACH

La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

(Art. 4, par. 1, GDPR)

ESEMPI DI DATA BREACH

Possono essere considerate violazioni di dati personali:

- Perdita dovuta ad un attacco informatico;
- Perdita accidentale (es. di una chiavetta o di un hard disk esterno);
- Allagamento;
- Incendio locali;
- Sottrazione di dati per furto di smartphone, tablet o pc;
- Accessi abusivi a sistemi informatici;
- Rapina, furto, danneggiamento delle strutture, dei contenuti o dei supporti informatici;
- Dipendenti infedeli che trafugano dati personali, li divulgano o li diffondono illecitamente;
- Lettura di dati da parte di persone non autorizzate dall'organizzazione.

ADMPIMENTI IN CASO DI DATA BREACH

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

(Art. 33, par. 1, GDPR)

QUANDO NON È NECESSARIO EFFETTUARE LA NOTIFICA

La notifica di violazione dei dati al Garante non è necessaria quando:

- ✓ *Il Titolare ha posto in essere tutte le misure tecniche ed organizzative adeguate di protezione e tali misure sono state applicate ai dati oggetto di violazione;*
- ✓ *Ha adottato tutte le misure atte a scongiurare il sopraggiungere di un rischio (no comunicazione agli interessati);*
- ✓ *La comunicazione richieda sforzi sproporzionati (no comunicazione agli interessati).*

LA COMUNICAZIONE AGLI INTERESSATI

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

Art. 34, GDPR

COME ORGANIZZARSI INTERNAMENTE?

- ✓ *PROCEDURA PER DATA BREACH*
- ✓ *REGISTRO DEGLI INCIDENTI DI SICUREZZA*

IL REGISTRO DELLE VIOLAZIONI

È un documento, sotto forma di scheda informativa, da compilare a seguito del rilevamento di una violazione di sicurezza dei dati personali che deve contenere:

- Data e ora dell'incidente e della sua rilevazione;
- Informazioni relative al soggetto che ha rilevato l'incidente;
- Descrizione dell'accaduto;
- Origine, dati coinvolti e sistemi oggetto dell'incidente;
- Modalità di risoluzione.

LA PRASSI NELLA REGIONE SICILIA

Il Titolare documenta qualsiasi violazione dei dati personali, comprese le circostanze in cui è avvenuto, le conseguenze ed i provvedimenti adottati per porvi rimedio (art.33); per tali fini ciascun Titolare tiene un registro delle violazioni dei dati, che include le violazioni avvenute presso il Responsabile, il sub-Responsabile e il sub-Responsabile tecnico coinvolti nei trattamenti di dati personali del Titolare.

LA PRASSI NELLA REGIONE SICILIA

Il Titolare documenta qualsiasi violazione dei dati personali, comprese le circostanze in cui è avvenuto, le conseguenze ed i provvedimenti adottati per porvi rimedio (art.33); per tali fini ciascun Titolare tiene un registro delle violazioni dei dati, che include le violazioni avvenute presso il Responsabile, il sub-Responsabile e il sub-Responsabile tecnico coinvolti nei trattamenti di dati personali del Titolare.

IL COORDINAMENTO DEL DPO

Al fine di catalogare unitariamente le violazioni il RPD coordina la realizzazione e il funzionamento di un sistema informativo per l'intera Amministrazione per la tenuta dell'elenco delle Violazioni di dati che sarà utilizzato dai Titolari e dai Responsabili e ne sorveglia l'aggiornamento.

IL COORDINAMENTO DEL DPO

Al fine di catalogare unitariamente le violazioni il RPD coordina la realizzazione e il funzionamento di un sistema informativo per l'intera Amministrazione per la tenuta dell'elenco delle Violazioni di dati che sarà utilizzato dai Titolari e dai Responsabili e ne sorveglia l'aggiornamento.

IL COORDINAMENTO DEL DPO

Inoltre al fine di rendere il più possibile omogenee le procedure seguite nell'Amministrazione regionale nei casi di violazioni di dati, il RPD propone una procedura operativa di risposta agli incidenti di sicurezza.

ATTENZIONE AL PHISHING!

COME DIFENDERSI DAL PHISHING

Effettuare un'analisi del testo: guardare alla semantica per capire se ci sono errori di battitura, errori grammaticali, se ci sembra un testo tradotto da un'altra lingua, se è stato ricevuto anche da colleghi, se c'è una frase di chiusura o meno, se è firmato da qualcuno.

Molti messaggi richiedono di cliccare su link che possono contenere malware o raccogliere credenziali su un sito clonato poiché la grafica apparirà esattamente la stessa del sito originale che già conosciamo.

Attenzione alle mail che richiedono l'apertura di un allegato da parte di un soggetto che non conosciamo.

COME DIFENDERSI DAL PHISHING

Mediante antivirus o sistemi di antiphishing. Questi sistemi possono segnalarci quando clicchiamo su un link che si tratta di un sito bollato come sito di phishing.

Attenzione! Non adagiarsi e non abbassare la guardia perché la sicurezza maggiore parte sempre dall'uomo.

Non tenere il segreto sugli attacchi subiti anche se possa suscitare vergogna. Piuttosto comunicarlo ai soggetti competenti per attivare la procedura di data breach.

DATA BREACH E SANZIONI DEI GARANTI EUROPEI

- L'Autorità danese ha sanzionato per € 14.000,00 un comune dopo che lo stesso ha subito il furto di un PC non criptato, su cui erano presenti i dati personali di oltre 20.620 cittadini residenti in città.

- L'Autorità danese ha sanzionato per € 7.000,00 un comune dopo che un suo dipendente ha subito il furto di PC portatile contenente i dati di oltre 1.600 dipendenti comunali. Tra i dati erano presenti dati sanitari e informazioni relative al numero di previdenza sociale.

DATA BREACH E SANZIONI DEI GARANTI EUROPEI

L'Autorità spagnola ha sanzionato per € 60.000,00 una società per lo smarrimento di 6 chiavette USB non cifrate che contenevano circa 11.000 dati personali di dipendenti.

L'Autorità ungherese ha sanzionato per € 1.500,00 la perdita di una flash memory.

DATA BREACH E SANZIONI DEI GARANTI EUROPEI

L’autorità inglese (ICO) ha sanzionato una compagnia aerea per oltre 200 milioni di euro in conseguenza di un data breach occorso al sito web della compagnia. Questo non era sufficientemente sicuro ed è stato oggetto di attacchi da parte di hacker con la compromissione dei dati di oltre 500.000 clienti.

NUOVI PERCORSI DI SVILUPPO
DELLA CAPACITÀ AMMINISTRATIVA
DELLA REGIONE SICILIANA

5 maggio 2021

GRAZIE PER L'ATTENZIONE!

Avv. Ernesto Belisario

e-lex STUDIO LEGALE

www.e-lex.it

Unione Europea
Repubblica Italiana
Regione Siciliana
FSE FONDO SOCIALE EUROPEO
SICILIA 2020
PROGRAMMA OPERATIVO
FormezPA