NUOVI PERCORSI DI SVILUPPO
DELLA CAPACITÀ AMMINISTRATIVA
DELLA REGIONE SICILIANA

31 maggio 2021

Avv. Ernesto Belisario

L'ACCOUNTABILITY DEL TITOLARE: ISTRUZIONI AGLI INCARICATI E BUONE PRATICHE

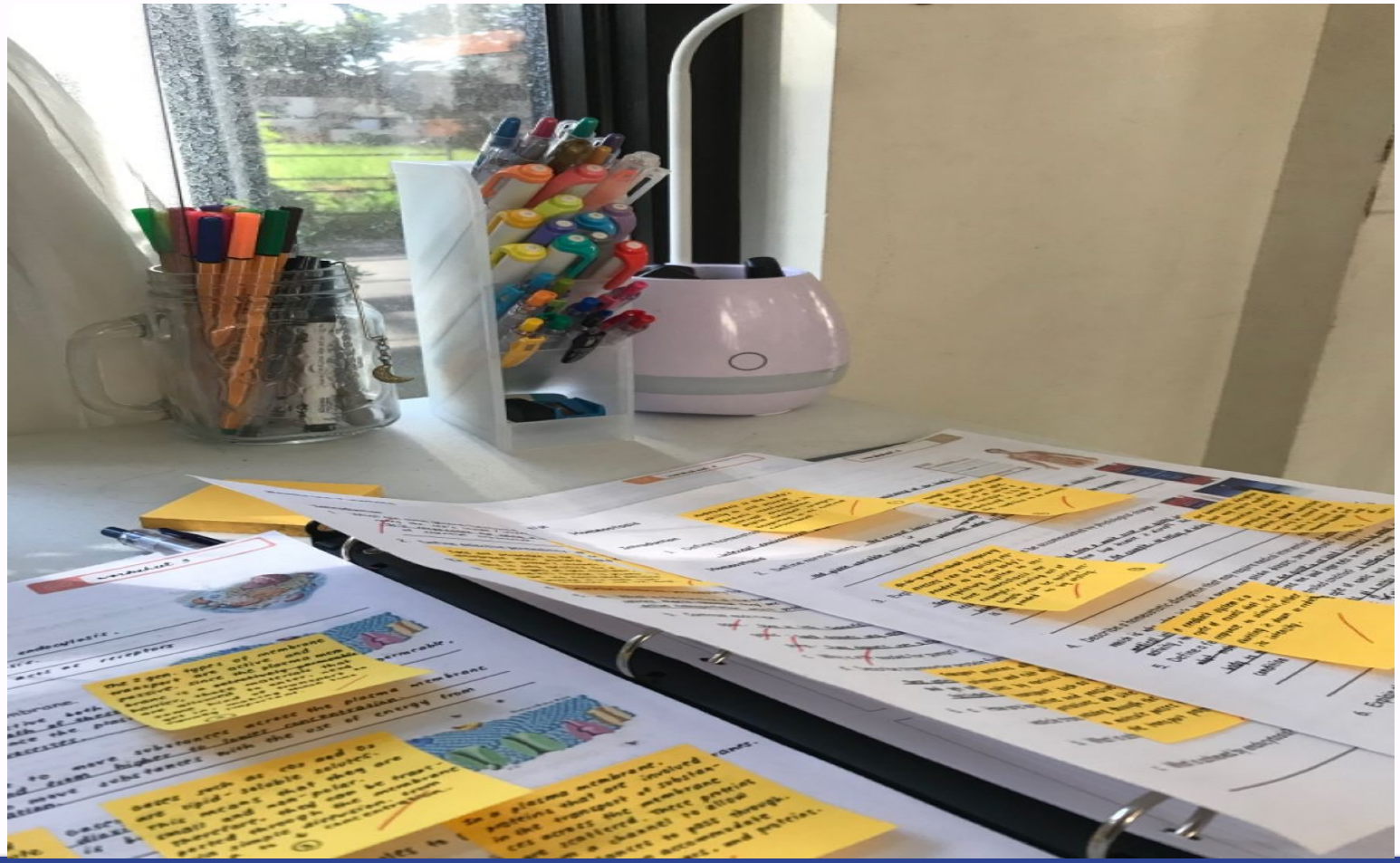
Unione Europea
Repubblica Italiana
Regione Siciliana
FSE FONDO SOCIALE EUROPEO
SICILIA 2020
PROGRAMMA OPERATIVO
FormezPA

Sommario


General Data
Protection Regulation

I – IL RUOLO DEGLI INCARICATI NELLA STRUTTRA DEL TITOLARE

RECAP



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».

È NECESSARIO UN ATTO FORMALE

Il titolare deve individuare con un **atto scritto** tutti i soggetti che, all'interno della propria struttura, sono chiamati a effettuare trattamenti di dati personali sotto la sua autorità.

All'interno dell'atto è opportuno specificare, nell'ambito delle mansioni proprie del dipendente, **quali saranno i trattamenti** che lo stesso sarà autorizzato a compiere.
Dovranno inoltre essere **elencate le specifiche istruzioni** per procedere a tale trattamento.

II – LE ISTRUZIONI AGLI INCARICATI NEL RISPETTO DEI PRINCIPI DI PRIVACY BY DESIGN E PRIVACY BY DEFAULT

LE ISTRUZIONI AGLI INCARICATI

L'accesso ai dati è consentito nella misura strettamente necessaria ad adempiere ai compiti assegnati, con divieto di qualunque diversa utilizzazione, funzione e divulgazione non espressamente autorizzata.

In particolare i soggetti autorizzati che trattano i dati per conto dell'Amministrazione osserveranno almeno le seguenti misure di sicurezza:

- è vietato comunicare a persone non autorizzate i dati personali di qualunque genere (giudiziari, sanitari o altri dati), elementi e informazioni dei quali il soggetto autorizzato viene a conoscenza nell'esercizio delle proprie funzioni e mansioni. In caso di dubbio, è necessario accertarsi che la persona a cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio dirigente.
- è vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base o altro
- la documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli atti e i documenti contenenti i dati personali, al termine dell'orario di lavoro, saranno riposti in cartelle ed armadi chiusi in modo da evitare che, in assenza degli autorizzati i soggetti non autorizzati ne possano prenderne visione;
- qualora i documenti contengano dati sensibili o giudiziari essi saranno riposti in archivio ad accesso controllato. I documenti contenenti dati sanitari, anche se pervenuti senza busta, saranno conservati in buste chiuse ed in armadi chiusi e, se trasmessi, andranno inseriti in buste chiuse con lettera di accompagnamento da cui non si evincano i dati sanitari in essa contenuti;
- per quanto riguarda i flussi di documenti cartacei all'interno degli uffici regionali, saranno adottate idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti in cartelle, carpette o buste chiuse ecc.);
- l'accesso ai dati tramite computer avverrà tramite un nome utente e una password associata attribuito al soggetto che effettua l'accesso;
- la password utilizzata deve essere di robustezza adeguata e contenere lettere maiuscole e minuscole, numeri e caratteri speciali. Non deve contenere elementi facilmente riconducibili all'utente;
- il nome utente e la password sono personali e non saranno condivisi con altri soggetti (a meno che non sia espressamente previsto);

LE ISTRUZIONI AGLI INCARICATI

LE ISTRUZIONI AGLI INCARICATI

accanto alle istruzioni fornite all'interno dell'atto di nomina, è importante predisporre un documento (**disciplinare**) che regoli la gestioni di:

- ✓ Documenti analogici
- ✓ Posta elettronica
- ✓ Navigazione in internet
- ✓ Utilizzo delle postazioni di lavoro
- ✓ Documenti informatici

DOCUMENTI ANALOGICI

In caso di trattamenti senza l'ausilio di strumenti tecnologici bisogna osservare le seguenti prescrizioni:

- Non lasciare incustoditi documenti contenenti dati personali;
- Evitare il deposito di questi documenti in luoghi di transito come corridoi o sale riunioni;
- Al termine della sessione di lavoro, ricollocare i documenti negli appositi cassetti e armadi dotati delle opportune misure di sicurezza;
- Non utilizzare promemoria volanti;
- Non usare questi documenti come carta per appunti.

POSTA ELETTRONICA

Quando il titolare mette a disposizione una casella di posta deve informare i propri dipendenti che questa può essere utilizzata esclusivamente per esigenze connesse all'attività lavorativa:

- Non è consentito utilizzare la casella per finalità personali;
- È vietato l'utilizzo di caselle di posta personali (gmail, live ecc) a meno che non siano state autorizzate;
- È fatto obbligo al dipendente di controllare la cartella spam con cadenza mensile.

POSTA ELETTRONICA

È vietato utilizzare la posta elettronica istituzionale per:

- Partecipare a forum o dibattiti non attinenti all'attività svolta per il Titolare;
- Inoltrare catene telematiche e altre forme di email che non abbiano attinenza con l'attività svolta;
- Allegare al testo delle comunicazioni materiale potenzialmente insicuro;
- Utilizzare tecniche di mail spamming per invio massiccio di comunicazioni a liste di utenti non istituzionali.

POSTA ELETTRONICA

- Nel caso in cui si riceva un'email da un mittente sospetto, per non correre il rischio di essere infettato da un virus, occorrerà cancellare il messaggio senza aprirlo;

- Nel caso in cui l'email sia inviata da un mittente conosciuto ma contenga allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd) questi ultimi non devono essere aperti.

NAVIGAZIONE IN INTERNET

- Non inserire i propri dati di login cliccando direttamente sui link proposti all'interno delle email, ma digitare l'indirizzo del sito manualmente per essere certi di non incorrere in siti contraffatti;

- Non cancellare la sottoscrizione ad una mailing list di cui non si è certi dell'iscrizione (potrebbe trattarsi di un raggiro da parte di uno spammer per ottenere conferme sulla validità dell'indirizzo email dell'utente).

UTILIZZO DELLA POSTAZIONE DI LAVORO

- In caso di non utilizzo o assenza temporanea, la postazione di lavoro dovrà essere bloccata tramite blocco manuale salvaschermo con richiesta di password al riavvio;

- In caso di assenza prolungata durante la giornata, è fatto obbligo di chiudere tutte le applicazioni dalle quali si ha accesso ai dati personali;

- Spegnere sempre la propria postazione di lavoro al termine dell'orario di lavoro.

"There are better ways to log off."

GESTIONE DELLE PASSWORD

Di norma:

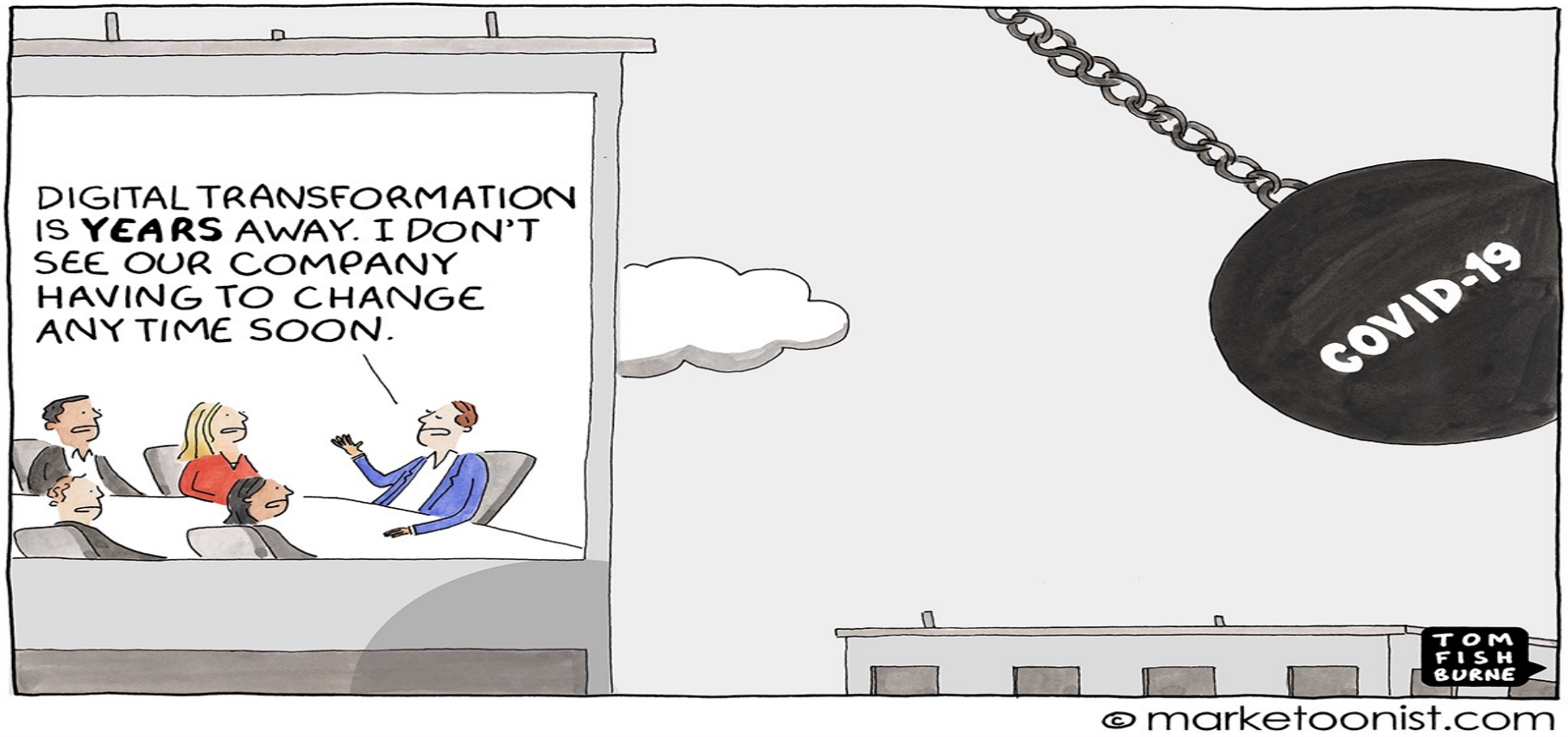
- La password deve essere sostituita al primo accesso, deve essere costituita da almeno 8 caratteri alfanumerici differenti, non deve contenere riferimenti (diretti o indiretti) riconducibili all'utente;
- Le password deve essere custodite con attenzione, non divulgate e non appuntate su fogli o post-it;
- Non utilizzare la funzione offerta da alcuni software di salvare la password per i successivi utilizzi;
- Non utilizzare email e password di un altro utente anche se fornita volontariamente o di cui si sia venuti a conoscenza casualmente;
- La password non deve mai essere divulgata a terzi neppure a coloro che telefonicamente si presentino come colleghi.

How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

STAMPA DI DOCUMENTI CONTENENTI DATI PERSONALI

È opportuno che non sia consentito accedere alle stampe persone non autorizzate; se la stampante si trova in stanze comuni o accessibili al pubblico, il dipendente deve recarsi quanto prima a ritirare le stampe. E se il documento contiene dati sensibili e/o giudiziari, prima di stamparli si devono usare opportune tecniche di oscuramento (es. barrare i dati sensibili presenti nel documento; sostituire i dati con delle “xxx”) e, in ogni caso, le operazioni di stampa devono essere effettuate alla presenza di una persona autorizzata.


DIGITAL TRANSFORMATION IS YEARS AWAY. I DON'T SEE OUR COMPANY HAVING TO CHANGE ANY TIME SOON.
COVID-19
TOM FISH BURNE
© marketoonist.com

LO SMART WORKING NELLA PA

CIRCOLARE N. 1/2020 DEL 4 MARZO DEL MINISTRO PER LA PA

LE INDICAZIONI ALLE AMMINISTRAZIONI

- Ricorso in via prioritaria a modalità flessibili di svolgimento della prestazione lavorativa
- Ricorso a strumenti per la partecipazione da remoto a riunioni e incontri di lavoro (videoconferenze e call conference)
- Utilizzo di soluzioni cloud per agevolare l'accesso condiviso a documenti, dati e informazioni
- Previsione di un sistema di reportistica interna da integrare con il sistema di misurazione e valutazione delle performance
- Ricorso a modalità flessibili per lo svolgimento della prestazione lavorativa anche mediante dispositivi personali del dipendente in caso di indisponibilità da parte della PA

www.lapadigitale.it

IL DECALOGO DELLO SMART WORKER

01 Assicurarsi che il sistema operativo del dispositivo sia aggiornato

02 Verificare che sia installato un antivirus e che sia aggiornato

03 Non memorizzare le password di accesso all'utilizzo delle risorse dell'ente sulle postazioni personali

04 Evitare di scrivere le password utilizzate su post-it e fogli lasciati in prossimità della postazione

05 Non effettuare salvataggi sui dispositivi personali e utilizzare preferibilmente le risorse in cloud messe a disposizione dall'amministrazione

06 Limitare il ricorso a USB pen e flash memory per archiviare dati e documenti

07 Bloccare la postazione in casi di assenza, seppur temporanea

08 Adottare ogni cautela a protezione del dispositivo utilizzato, specialmente in caso di spostamenti

09 Non gettare nella spazzatura documenti cartacei utilizzati per l'attività lavorativa contenenti dati personali se non dopo averli triturati

10 Comunicare senza ritardo ogni tipo di incidente da cui potrebbe derivare una violazione di dati personali

www.lapadigitale.it

Smart working:
il vademecum per lavorare online in sicurezza

AGID | Agenzia per l'Italia Digitale

LE PRINCIPALI REGOLE DA OSSERVARE

- in caso di uso promiscuo del dispositivo, creare un'apposita utenza;
- prestare massima attenzione ai contenuti delle mail per evitare di incorrere in truffe digitali;
- conservare accuratamente i documenti cartacei contenenti dati personali utilizzati per l'attività;
- non utilizzare Whatsapp per inoltrare ai colleghi dati personali di utenti o propri interlocutori o per trasmettere ai propri interlocutori documenti contenenti dati personali;
- non lasciare incustoditi i dispositivi utilizzati per l'attività lavorativa;
- in caso di utilizzo di un dispositivo personale è possibile prevedere un check da remoto da parte dell'AdS per verificare che tutti i parametri siano aggiornati;
- utilizzare una connessione cifrata: il router deve avere una password robusta. Se possibile modificare user e password.

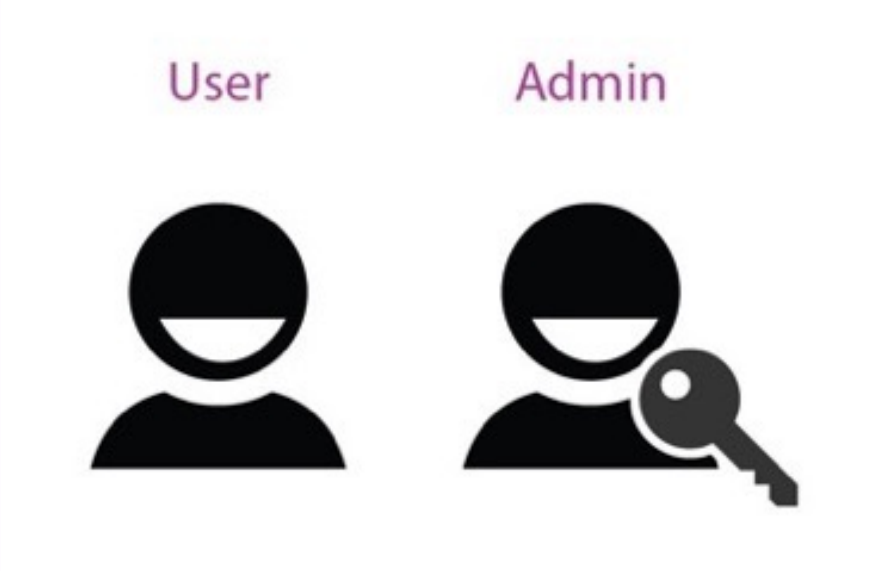
III – GLI AMMINISTRATORI DI SISTEMA

NUOVI PERCORSI DI SVILUPPO
DELLA CAPACITÀ AMMINISTRATIVA
DELLA REGIONE SICILIANA

FormezPA

L'AMMINISTRATORE DI SISTEMA

L'Amministratore di Sistema è un operatore preposto all'esercizio dei sistemi informatici che occupa il vertice della gerarchia di utenze in termini di privilegi di accesso alle risorse informatiche e ai dati ivi custoditi.



MISURE ATTUATIVE

- delineare e dettare le procedura di nomina e di attribuzione delle funzioni degli amministratori di sistema;
- delineare gli adempimenti in materia di protezione dei dati personali;
- dettare specifiche misure e cautele in riferimento alle mansioni svolte.

Riferimenti normativi:

- GDPR (Regolamento UE 2016/679) e Codice Privacy (D. Lgs. n. 196/2003);
- Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008.

FUNZIONI, RUOLO E REQUISITI

- Monitorare l'infrastruttura informatica di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
- Introdurre ed integrare nuove tecnologie negli ambienti esistenti;
- Installare e configurare nuovo hardware/software sia lato client sia lato server;
- Applicare le patch e gli aggiornamenti necessari ai software di base ed applicativi;
- Gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione;
- Fornire risposte alle questioni tecniche sollevate dall'utenza, porre rimedio ai problemi/guasti tramite tecniche di troubleshooting;
- Pianificare e verificare la corretta esecuzione dei backup e delle repliche;
- Ottenere le migliori prestazioni possibili con l'hardware a disposizione;
- Operare secondo le prescrizioni di sicurezza e le procedure interne previste.

COMPITI PRINCIPALI

PROFILI DI AUTORIZZAZIONE

In base alle attività da eseguire, ciascun amministratore rivestirà un ruolo al quale corrisponde un determinato profilo di autorizzazione.

OUTSOURCING

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

REQUISITI DI IDONEITÀ E CARATTERISTICHE DEGLI ADS

L’attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell´esperienza, della capacità e dell’affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

DESIGNAZIONE INDIVIDUALE

La designazione quale amministratore di sistema deve essere in ogni caso **individuale** e recare l´elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

RAPPORTI CON IL TITOLARE

L’operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un’attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

IDENTIFICAZIONE E TRACCIAMENTO DEGLI ACCESSI LOGICI

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

IV – IL QUADRO SANZIONATORIO DEL GDPR

IL SISTEMA SANZIONATORIO

NUOVI PERCORSI DI SVILUPPO
DELLA CAPACITÀ AMMINISTRATIVA
DELLA REGIONE SICILIANA

FormezPA

IL SISTEMA SANZIONATORIO

Il GDPR definisce un impianto sanzionatorio molto più rigido di quello previsto dal Codice Privacy:

- *sono previste sanzioni amministrative fino a 20 milioni di Euro;*
- *è prevista la responsabilità civile nei confronti dell'interessato che subisca un danno materiale o immateriale causato da una violazione del GDPR;*
- *sanzioni penali possono essere previste dal legislatore nazionale.*

SANZIONI AMMINISTRATIVE

fino a 20 milioni di euro, in caso di violazione delle disposizioni in materia di:

- principi di base del trattamento, comprese le condizioni relative al consenso; diritti degli interessati;
- trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
- inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

SANZIONI AMMINISTRATIVE

fino a 10 milioni di euro, in caso di violazione delle disposizioni in materia di:

- obblighi del titolare del trattamento e del responsabile del trattamento;
- obblighi dell'organismo di certificazione; obblighi dell'organismo di controllo.

PRINCIPIO DI PROPORZIONALITÀ

Le sanzioni amministrative sono comminate dall'autorità di controllo sulla base delle seguenti circostanze (art. 83, par. 2, GDPR):

- la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- il carattere doloso o colposo della violazione;
- le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

PRINCIPIO DI PROPORZIONALITÀ

Le sanzioni amministrative sono comminate dall'autorità di controllo sulla base delle seguenti circostanze (art. 53, par. 2, GDPR):

- il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto;
- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

PRINCIPIO DI PROPORZIONALITÀ

Le sanzioni amministrative sono comminate dall'autorità di controllo sulla base delle seguenti circostanze (art. 53, par. 2, GDPR):

- le categorie di dati personali interessate dalla violazione;
- la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- qualora siano stati precedentemente disposti provvedimenti nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

PRINCIPIO DI PROPORZIONALITÀ

Le sanzioni amministrative sono comminate dall'autorità di controllo sulla base delle seguenti circostanze (art. 53, par. 2, GDPR):

- le categorie di dati personali interessate dalla violazione;
- la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- qualora siano stati precedentemente disposti provvedimenti nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

PRINCIPIO DI PROPORZIONALITÀ

Le sanzioni amministrative sono comminate dall'autorità di controllo sulla base delle seguenti circostanze (art. 53, par. 2, GDPR):

- l'adesione ai codici di condotta approvati ai sensi dell'articolo o ai meccanismi di certificazione;
- eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

PROFILI RISARCITORI

Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

Art. 82, par. 1, GDPR

PROFILI RISARCITORI

Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Art. 82, par. 2 e 3, GDPR

TRATTAMENTO ILLECITO DI DATI

Chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.

Art. 167, comma 1, D. Lgs. n. 196/2003

COMUNICAZIONE E DIFFUSIONE ILLECITA DI DATI PERSONALI

Chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.

Art. 167-bis, comma 1, D. Lgs. n. 196/2003

ACQUISIZIONE FRAUDOLENTA DI DATI

Chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.

Art. 167-ter, comma 1, D. Lgs. n. 196/2003

FALSITÀ NELLE DICHIARAZIONI AL GARANTE

Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.

Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

Art. 168, commi 1 e 2, D. Lgs. n. 196/2003

RESPONSABILITÀ ERARIALE

La responsabilità erariale sussiste, inoltre, in tutti i casi in cui le nuove tecnologie siano utilizzate in modo scorretto: basti pensare alla mancata adozione delle cautele di sicurezza previste dalla normativa in materia di riservatezza di dati personali
(artt. 31 ss, D.lgs. n. 196/2003) che abbia determinato un risarcimento al privato danneggiato, oppure l'assenza di procedure di controllo che abbia determinato un danno diretto alle casse dell'Ente

Corte Conti, Reg. Toscana, 26 aprile 2006, n. 265

RESPONSABILITÀ ERARIALE

Il pagamento della sanzione irrogata dal Garante Privacy costituisce danno erariale.

(Corte Conti, Sezione giurisdizionale per il Lazio, Sentenza 28 maggio 2019, n. 246).

RESPONSABILITÀ ERARIALE

Le sanzioni pecuniarie del Garante Privacy costituiscono danno erariale.

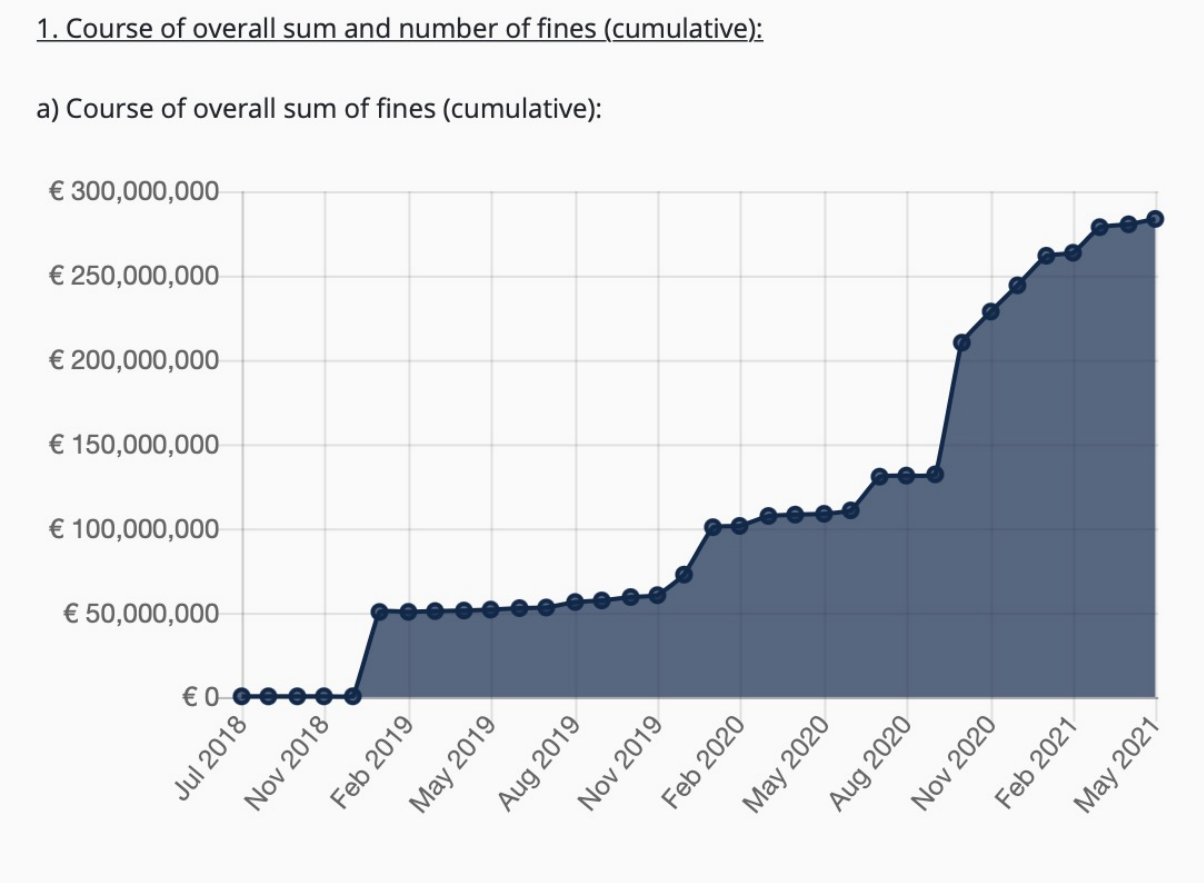
- ✓ Corte Conti, sezione Giurisdizionale Calabria, con la sentenza n. 429/2019 (condannato il Presidente della Regione per mancato rispetto delle misure di sicurezza e per tardivo riscontro a una richiesta del Garante);
- ✓ Corte Conti, sezione Giurisdizionale Lazio, con la sentenza n. n. 246/2019 (condannato Dirigente scolastico per la pubblicazione online di una circolare contente dati di alunni disabili);
- ✓ Corte Conti, sezione Giurisdizionale Toscana, con la sentenza n. n. 445/2019 (condannato Commissario straordinario per mancata nomina di un responsabile esterno).

V – LE SANZIONI DEI GARANTI EUROPEI

NUOVI PERCORSI DI SVILUPPO
DELLA CAPACITÀ AMMINISTRATIVA
DELLA REGIONE SICILIANA

FormezPA

L'AUMENTO DEL NUMERO DI SANZIONI



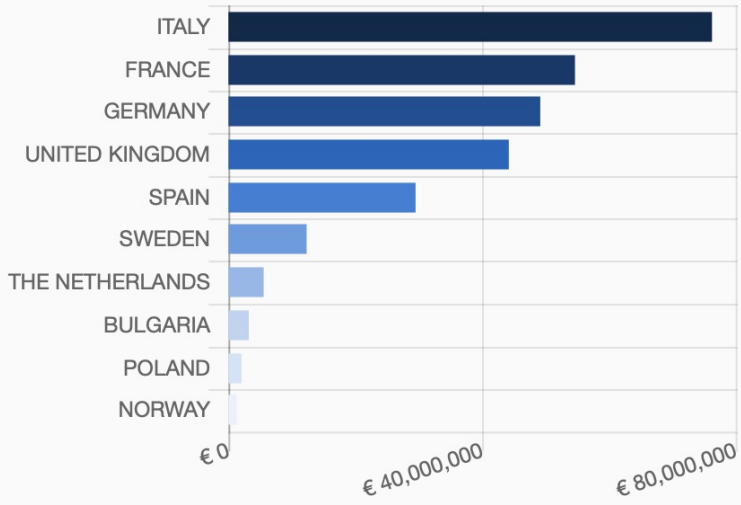
enforcementtracker.com, provided by CMS Law.Tax

LE SANZIONI NEGLI STATI MEMBRI

Statistics: Countries with highest fines (Top 10)
The following statistics show how many fines and what sum of fines have been imposed per country to date (only top 10 countries).

Note: Only fines with valid information on the amount of the fine are taken into account.

1. By total sum of fines:



	Country	Sum of Fines
	ITALY	**€ 76,271,601** (at 77 fines)
	FRANCE	**€ 54,661,300** (at 14 fines)
	GERMANY	**€ 49,186,833** (at 30 fines)
	UNITED KINGDOM	**€ 44,221,000** (at 4 fines)
	SPAIN	**€ 29,519,410** (at 229 fines)
	SWEDEN	**€ 12,332,430** (at 17 fines)
	THE NETHERLANDS	**€ 5,552,500** (at 12 fines)
	BULGARIA	**€ 3,210,690** (at 20 fines)
	POLAND	**€ 2,061,498** (at 24 fines)
	NORWAY	**€ 1,316,550** (at 27 fines)

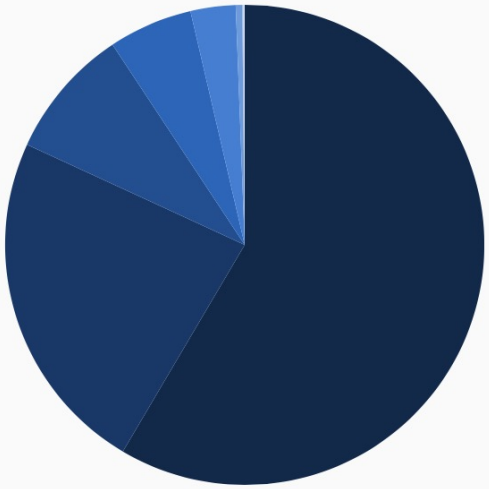
enforcementtracker.com, provided by CMS Law.Tax

LE VIOLAZIONI PIÙ FREQUENTI

Statistics: Fines by type of violation
The following statistics show how many fines and what sum of fines have been imposed per type of GDPR violation to date.

Note: Only fines with valid information on the amount of the fine and on the type of violation are taken into account.

1. By total sum of fines:



Violation	Sum of Fines
Insufficient legal basis for data processing	**€ 166,615,243** (at 248 fines)
Insufficient technical and organisational measures to ensure information security	**€ 66,547,219** (at 147 fines)
Non-compliance with general data processing principles	**€ 25,179,664** (at 120 fines)
Insufficient fulfilment of data subjects rights	**€ 16,131,025** (at 66 fines)
Insufficient fulfilment of information obligations	**€ 8,665,195** (at 39 fines)
Insufficient fulfilment of data breach notification obligations	**€ 1,245,791** (at 18 fines)
Insufficient cooperation with supervisory authority	**€ 186,729** (at 27 fines)
Lack of appointment of data protection officer	**€ 186,000** (at 5 fines)
Insufficient data processing agreement	**€ 89,380** (at 3 fines)
Unknown	**€ 500** (at 1 fines)

enforcementtracker.com, provided by CMS Law.Tax

PROFILI DI AUTORIZZAZIONE

L'Autorità Belga ha sanzionato per 100.000 € un istituto bancario che non aveva adottato adeguate misure per prevenire accessi non autorizzati da parte degli stessi dipendenti.
A causa di ciò è accaduto che una dipendente accedesse illecitamente, oltre 20 volte, ai dati finanziari dell'ex marito, per usare poi queste informazioni nella causa di divorzio.

PROFILI DI AUTORIZZAZIONE

- L'autorità olandese ha sanzionato per € 460.000,00 un ospedale per la gestione non corretta dei fascicoli dei pazienti. Molti dipendenti avevano curiosato nella cartella clinica di una persona vip ricoverata presso l'ospedale.
- L'autorità 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.
- L'Autorità tedesca ha sanzionato per € 105.000,00 un ospedale per la pratica di patient mix up a causa di gravi lacune nel management dei pazienti. Nella pratica venivano mescolati i dati di pazienti in fascicoli di altri pazienti.
- L'Autorità italiana ha sanzionato per € 30.000,00 l'Azienda Ospedaliero Universitaria Integrata di Verona 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.

VIOLAZIONE DEL PRINCIPIO DI LIMITAZIONE

L'Autorità olandese per la protezione dei dati ha sanzionato una compagnia assicurativa operante nel settore medico, per violazione dell'art. 5 del Regolamento, in quanto i membri dello staff del marketing avevano libero accesso ai dati clinici dei pazienti.

Questa palese violazione degli artt. 5 e 25 del Regolamento ha portato a una sanzione di 50.000 euro.

ATTENZIONE ALL'UTILIZZO DELLA MAIL

L'Autorità islandese ha sanzionato una scuola per € 9.000,00 in quanto un docente ha inviato via mail agli studenti e ai genitori un allegato contenente il rendimento scolastico degli alunni, senza adottare le cautele necessarie e quindi senza adottare adeguate misure di sicurezza.

L'Autorità spagnola ha sanzionato per € 3.600,00 un titolare che ha inviato il contenuto di una busta paga al dipendente sbagliato.

L'Autorità italiana ha ammonito una Provincia per aver inviato senza utilizzare il campo copia nascosta una mail a sedici genitori di bambini non in regola con l'obbligo di vaccinazione. Il Garante ha precisato che le informazioni contenute nella comunicazione della Provincia sono qualificabili come dati relativi alla salute dei minori. Il Garante ha tenuto conto del fatto che fosse stata la Provincia a segnalare la disattenzione del dipendente nell'invio di queste comunicazioni con indirizzi in chiaro precisando di aver inviato delle mail di scuse ai destinatari.

ATTENZIONE ALL'INVIO DI MAILING LIST: UTILIZZARE SEMPRE IL CAMPO CCN

L'Autorità spagnola per la protezione dei dati (AEPD) ha sanzionato una società per aver mal gestito l'invio di comunicazioni marketing. La società infatti utilizzava una mailing list in cui gli indirizzi di posta erano visibili, in chiaro, a tutti i destinatari. Ciò ha determinato l'ostensione degli indirizzi mail (che sono dati personali!!), a tutti i componenti della mailing list.

Questa comportamento è stato configurato come violazione dell'art. 5, par. 1, lett. f) del GDPR ha portato a una sanzione di 36.000 euro.

IL CORRETTO UTILIZZO DEL CAMPO CCN

Nel caso di invio di mail a più destinatari (come nel caso dell'utilizzo di una mailing list) è necessario utilizzare il campo CCN, di modo da evitare la divulgazione dei contatti mail.

È molto importante, in questo senso, procedere ad una sensibilizzazione dei dipendenti che potrebbero non conoscere la differenza tra CC e CCN.

CARENTI MISURE ORGANIZZATIVE

L'Autorità cipriota ha sanzionato per 15.000 € un istituto assicurativo pubblico per plurime violazioni del GDPR emerse a seguito di una richiesta di accesso da parte di un interessato. In particolare, il Titolare aveva smarrito il contratto assicurativo con l'interessato. Ciò ha comportato:

- l'impossibilità per l'interessato di esercitare il proprio diritto di accesso;
- l'emersione di inadeguate misure di sicurezza e organizzative;
- la mancata denuncia del relativo data breach;
- la violazione dell'obbligo di protezione dei dati personali (art. 5, par. 1, lett. f GDPR).

CARENTI MISURE ORGANIZZATIVE

Il Garante italiano ha sanzionato un Comune per 40.000 € per la mancata adozione di misure tecniche e organizzative adeguate.
In particolare, il caso è venuto alla luce a seguito di un reclamo proposto da un interessato, i cui dati dati relativi ad una richiesta di sussidio erano stati trattati da soggetti non autorizzati e per fini personali.

CARENTI MISURE ORGANIZZATIVE

L'Autorità ungherese ha sanzionato un ente pubblico in quanto lo stesso ha comunicato, a mezzo mail, i risultati di test covid rapidi, unitamente ai nomi dei pazienti e ai loro dati di contatto, inserendo le informazioni all'interno di un documento excel non criptato e senza alcuna misura per garantire la confidenzialità delle informazioni.

FOCUS: REGISTRO DEL TRATTAMENTO E BASI GIURIDICHE

REGISTRO DEL TRATTAMENTO E BASE GIURIDICA

RECAP

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) *l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;*

b) *il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;*

c) *il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;*

BASE GIURIDICA

d) *il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;*

e) *il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;*

f) *il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.*

BASE GIURIDICA

La base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.

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

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)

COME COMPILARE IL REGISTRO

L'indicazione della base giuridica in corrispondenza delle singole attività di trattamento, **non è un elemento necessario** richiesto dal GDPR.

Si tratta però di un'informazione molto importante, sia nell'ottica di «tracciare» correttamente tutti i trattamenti e verificare che gli stessi siano coperti da un adeguato presupposto di liceità, sia nel momento della redazione delle informative privacy, in quanto il registro così compilato consente di avere a disposizione ogni elemento necessario.

Il titolare, al momento di procedere ad un trattamento di dati personali, deve sempre interrogarsi su quale sia (e **se** vi sia) una condizione che rende **lecito** quel trattamento.

NUOVI PERCORSI DI SVILUPPO
DELLA CAPACITÀ AMMINISTRATIVA
DELLA REGIONE SICILIANA

31 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