



ISTITUTO D'ISTRUZIONE SECONDARIA SUPERIORE

De Rogatis - Fioritto

Via Marconi - Villaggio studentesco "Dr. V. Zaccagnino" - 71015 San Nicandro Garganico (FG)

Tel. 0882/472582 Fax 0882/476525

Sito Web: www.derogatisfioritto.gov.it



Ai Docenti
Al personale Ata
Al DSGA

Sede di San Nicandro Garganico
Sede di Cagnano Varano

ALBO

FGIS007003-GDPR-005/B

OGGETTO: *Pubblicazione Codice di comportamento in materia di trattamento dei dati personali (incaricati) - docenti.*

Si comunica che in data odierna (16/05/2019) viene pubblicato all'albo dell'Istituto e sul sito web www.derogatisfioritto.gov.it in apposita sezione il Codice di comportamento di cui all'oggetto.

IL DIRIGENTE SCOLASTICO
Prof. Francesco DONATACCIO

Firma autografa sostituita a mezzo stampa ai sensi
dell'art. 3, comma 2, del decreto Legislativo n. 39/1993



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)

CODICE DI COMPORTAMENTO IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

(ai sensi del Regolamento UE 2016/679 e del D.Lgs. n. 196/2003 e s.m.i.)



IISS DE ROGATIS - FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)



DOCENTI

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)

Premessa

Il Regolamento UE 2016/679 ha modificato la normativa in materia di protezione dei dati personali introducendo importanti novità in materia ed uniformando la normativa all'interno dell'UE.

Una delle principali innovazioni consiste nel c.d. PRINCIPIO DI ACCOUNTABILITY (responsabilizzazione) che impone a chiunque tratti dati personali di impostare un sistema di trattamento di dati tale che sia possibile dimostrare di aver ottemperato a tutte le disposizioni previste dal Regolamento.

Con il D.Lgs. 101/2018 il D.Lgs. n. 196/2003 è stato armonizzato alla nuova normativa europea.

Tutta la documentazione (atti normativi, regolamenti applicativi, Provvedimenti del Garante, Linee Guida ecc.) sono disponibili e liberamente scaricabili dal sito internet del Garante per la Protezione dei Dati Personali www.garanteprivacy.it.

Principi generali

Tutte le disposizioni del Regolamento ruotano attorno ad alcuni principi di base che devono essere rispettati per ogni trattamento. Nella seguente immagine vengono riportati detti principi:



Organigramma per la Protezione dei Dati Personali

Come previsto nel Regolamento UE 2016/679, all'interno dell'Istituto Scolastico sono stati individuati i vari soggetti coinvolti nella Protezione dei dati Personali: i relativi riferimenti sono stati riportati nell'atto di designazione. Ogni variazione verrà comunicata formalmente.

Riservatezza e rispetto del Segreto Professionale

I dipendenti sono tenuti alla riservatezza sulle informazioni di cui vengono a conoscenza nell'esercizio delle proprie funzioni (art. 326 del c.p. ed art. 15 del DPR 3/1957 ed art. 28 della Legge 241/1990 e del Codice di Comportamento di cui al Decreto 16/4/2013 n. 62), anche dopo la cessazione dell'incarico. A tal fine giova ricordare che ogni dipendente pubblico dovrebbe spontaneamente e senza imposizione rispettare i principi di

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)

riservatezza in quanto strettamente connessi ai doveri minimi di diligenza, lealtà, imparzialità e buona condotta. A tal fine si riporta uno stralcio dell'articolo 12 del D.P.R. n. 62/2013, a cui si fa comunque riferimento per tutto quanto concerne la condotta in ambito lavorativo: *Art. 12 - Rapporti con il pubblico: 1. Il dipendente in rapporto con il pubblico si fa riconoscere attraverso l'esposizione in modo visibile del badge od altro supporto identificativo messo a disposizione dall'amministrazione, salvo diverse disposizioni di servizio, anche in considerazione della sicurezza dei dipendenti, opera con spirito di servizio, correttezza, cortesia e disponibilità e, nel rispondere alla corrispondenza, a chiamate telefoniche e ai messaggi di posta elettronica, opera nella maniera più completa e accurata possibile. Qualora non sia competente per posizione rivestita o per materia, indirizza l'interessato al funzionario o ufficio competente della medesima amministrazione. Il dipendente, fatte salve le norme sul segreto d'ufficio, fornisce le spiegazioni che gli siano richieste in ordine al comportamento proprio e di altri dipendenti dell'ufficio dei quali ha la responsabilità od il coordinamento. Nelle operazioni da svolgersi e nella trattazione delle pratiche il dipendente rispetta, salvo diverse esigenze di servizio o diverso ordine di priorità stabilito dall'amministrazione, l'ordine cronologico e non rifiuta prestazioni a cui sia tenuto con motivazioni generiche. Il dipendente rispetta gli appuntamenti con i cittadini e risponde senza ritardo ai loro reclami. 2. Salvo il diritto di esprimere valutazioni e diffondere informazioni a tutela dei diritti sindacali, il dipendente si astiene da dichiarazioni pubbliche offensive nei confronti dell'amministrazione. Omissis...4. Il dipendente non assume impegni né anticipa l'esito di decisioni o azioni proprie o altrui inerenti all'ufficio, al di fuori dei casi consentiti. Fornisce informazioni e notizie relative ad atti od operazioni amministrative, in corso o conclusi, nelle ipotesi previste dalle disposizioni di legge e regolamentari in materia di accesso, informando sempre gli interessati della possibilità di avvalersi anche dell'Ufficio per le relazioni con il pubblico. Rilascia copie ed estratti di atti o documenti secondo la sua competenza, con le modalità stabilite dalle norme in materia di accesso e dai regolamenti della propria amministrazione. 5. Il dipendente osserva il segreto d'ufficio e la normativa in materia di tutela e trattamento dei dati personali e, qualora sia richiesto oralmente di fornire informazioni, atti, documenti non accessibili tutelati dal segreto d'ufficio o dalle disposizioni in materia di dati personali, informa il richiedente dei motivi che ostano all'accoglimento della richiesta. Qualora non sia competente a provvedere in merito alla richiesta cura, sulla base delle disposizioni interne, che la stessa venga inoltrata all'ufficio competente della medesima amministrazione.* Per "informazioni riservate" si intendono tutte le informazioni di qualsivoglia natura riferite o apprese in occasione dello svolgimento delle proprie mansioni. Ogni dipendente deve preservare dati, notizie ed informazioni riferite all'attività della Pubblica Amministrazione dalla conoscibilità di terzi soggetti non espressamente autorizzati ad averne notizia. I comportamenti contrari a quanto sopra specificato sono punibili ai sensi dell'articolo 16 del D.P.R. citato.

Trattamento dei Dati con strumenti elettronici

- Il trattamento dei dati personali con strumenti elettronici è consentito esclusivamente all'interno dell'Istituto Scolastico ed utilizzando gli strumenti elettronici messi a disposizione dell'Istituto Scolastico. L'eventuale utilizzo degli strumenti personali deve essere preventivamente autorizzato dal Titolare del trattamento ferma restando la responsabilità del proprietario per violazione o perdita di dati legati al cattivo funzionamento dello strumento utilizzato
- È vietato costruire "banche dati" ulteriori rispetto a quelle presenti nell'Istituto Scolastico: qualora l'acquisizione dei dati sia necessaria per lo svolgimento dell'attività didattica, tutte le informazioni devono essere richieste agli uffici di segreteria preposti
- In caso di affidamento di incarichi specifici che richiedano l'accesso a banche dati diverse e normalmente non trattate nell'esercizio della propria funzione, si procederà a specifico incarico

Registro elettronico

Il Registro elettronico si configura come ATTO PUBBLICO, per cui il docente, nella sua compilazione, è passibile delle sanzioni penali previste dagli articoli 476 (Falso ideologico in atto pubblico) e 479 (Falso materiale in atto pubblico) del c.p.p.

La sua compilazione deve avvenire nel minor tempo possibile senza procrastinare l'inserimento delle informazioni a momenti successivi.

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)

L'utilizzo di strumenti personali per l'accesso al Registro Elettronico deve essere preventivamente autorizzato dal TITOLARE DEL TRATTAMENTO DEI DATI.

Le credenziali di accesso devono ritenersi riservate: il docente è personalmente responsabile della custodia delle proprie credenziali per l'accesso allo strumento e deve seguire tutte le cautele previste sia per la custodia delle passwords, sia per la costruzione delle stesse (vedere Linee guida allegate).

Trattamento dei Dati con strumenti cartacei

- L'acquisizione dei dati contenuti in documenti che la scuola deve o intende trattare deve essere effettuata solo dagli addetti specificamente incaricati al trattamento stesso: l'insegnante NON PUO' acquisire dati personali di alcun genere, salvo preventiva e specifica autorizzazione del Dirigente Scolastico
- non è altresì consentita la creazione e gestione di banche dati ulteriori rispetto a quelle presenti negli uffici amministrativi
- non è consentito redigere per proprio conto moduli di raccolta dati per autorizzazioni di vario genere, informative ecc.; tutta la documentazione in materia di protezione dei dati personali è gestita dagli uffici amministrativi ai quali ci si dovrà rivolgere per tutte le esigenze di acquisizione e/o trattamento dei dati
- è vietato l'utilizzo di informative parziali, modificate senza la preventiva autorizzazione del titolare del trattamento, non codificate, non aggiornate o comunque redatte senza il controllo del titolare del trattamento. È vietato predisporre moduli di acquisizione dati autonomamente, senza che sia stata preventivamente valutata la liceità del trattamento (base giuridica) nonché il rispetto di tutti gli altri principi del trattamento e senza che siano stati redatti, codificati e controllati la specifica informativa e l'eventuale consenso
- in caso di acquisizione di documenti contenenti dati "particolari" (sensibili) in particolare quelli relativi allo stato di salute, il docente dovrà provvedere all'acquisizione e conservazione in forma tale da proteggerne il contenuto fino alla consegna agli uffici preposti
- le stesse disposizioni di cui al precedente punto dovranno essere seguite per l'acquisizione di documenti contenenti dati "particolari" (sensibili) diversi da quelli sanitari
- l'acquisizione dei dati dei minorenni dovrà essere effettuata direttamente dai genitori o dai tutori: non è ammessa l'acquisizione di dati resi da soggetti diversi. L'informativa al trattamento dei dati di minori dovrà essere resa ad entrambi i genitori che provvederanno entrambi alla sottoscrizione dell'eventuale consenso e/o liberatoria. In caso di impossibilità di uno dei due genitori sarà possibile accettare informative e consensi/liberatorie sottoscritte da un solo genitore solo se accompagnate da specifica DICHIARAZIONE SULLA RESPONSABILITA' GENITORIALE.
- è fatto divieto di acquisire in chiaro dati personali se le finalità istituzionali consentono la loro acquisizione in forma anonima
- è vietato accedere agli uffici amministrativi senza previa autorizzazione del titolare del trattamento o comunque al di là degli orari di ricevimento stabiliti
- è vietato accedere agli archivi cartacei ed elettronici senza previa autorizzazione del titolare del trattamento
- ogni documento consegnato "brevi manu" da soggetti esterni e contenente dati personali deve essere immediatamente riposto in busta chiusa sulla quale specificare il destinatario del documento (es. DS, DSGA ecc.)
- in generale ogni prodotto dell'elaborazione di dati personali, anche se non costituisce documento definitivo (ad es. appunti, stampe di prova, bozze, stampe interrotte ecc.) deve essere trattato con le stesse cautele e seguendo le stesse regole riservate alla versione definitiva
- è vietato portare fuori dall'Istituto Scolastico atti e/o documenti contenenti dati personali se non previa esplicita e documentata autorizzazione

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)

- quando è necessario fotocopiare documenti contenenti dati personali (e/o particolari), deve procedervi direttamente il soggetto incaricato che provvederà a presidiare l'area di fotocopiatura ed a prelevare immediatamente sia l'originale che la/copia/e in modo da evitare che le stesse siano anche solo accidentalmente visibili; in caso di copie da cestinare, queste vanno distrutte in modo da essere non più leggibili
- la movimentazione dei documenti all'esterno, deve essere preceduta da un'accurata fase di protezione dei documenti, mediante utilizzo di buste chiuse, opache e sigillate. La movimentazione di più documenti deve essere effettuata in modo da ridurre al minimo il rischio di smarrimento o perdita accidentale dei documenti, mediante utilizzo di cartelle o contenitori o borse tali da evitare lo scivolamento dei documenti dal contenitore
- prima dell'accesso del personale addetto alla pulizia dei locali in cui sono custoditi e lavorati documenti contenenti dati personali, è necessario richiudere tutta la documentazione e spegnere i PC in modo da evitare l'accesso accidentale a dati per i quali si soggetti non hanno autorizzazione al trattamento. Qualora le attività di pulizia debbano essere eseguite nell'impossibilità di archiviare in modo sicuro i documenti contenenti dati, un addetto amministrativo deve presiedere durante tutte le attività. Le stesse cautele devono essere seguite per l'accesso agli archivi ed in tutti i locali in cui sono detenuti, anche solo provvisoriamente, documenti contenenti dati personali. Le stesse cautele devono essere seguite anche in caso di accesso di soggetti terzi addetti alla manutenzione di locali ed attrezzature.
- prima di procedere accertarsi che il trattamento rientri nell'esercizio delle proprie funzioni istituzionali e che il la comunicazione/diffusione sia prevista ed autorizzata
- per la consegna cartacea a mano di documenti cartacei in uscita è necessario, verificate le necessarie autorizzazioni e la possibilità che tale documento sia consegnato all'esterno, che lo stesso sia custodito in busta chiusa opaca e che la persona a cui il documento sia consegnato sia il destinatario della documentazione
- per la spedizione del formato elettronico è necessario adottare le cautele finalizzate alla possibilità che il documento venga inviato per errore a destinatario diverso a causa, ad esempio, di una non corretta digitazione dell'indirizzo.
- tutti i terzi che chiedano il rilascio di documento devono essere stati preventivamente autorizzati

Per ogni dubbio rivolgersi al Titolare del Trattamento.

Social e trattamento dei dati

L'utilizzo dei social nella vita quotidiana ha sicuramente apportato un valore aggiunto nella comunicazione e nella velocità di circolazione delle informazioni. L'utilizzo di pagine facebook, instagram, twitter ecc. o dei "gruppi whatsapp" costituisce sicuramente uno strumento che potrebbe rivelarsi positivo nell'ottica della circolazione delle informazioni. Tuttavia, a tutela dei dati personali dei soggetti interessati, è necessario limitare l'utilizzo di tali strumenti. Pertanto:

- è vietato aprire, a nome dell'Istituto Scolastico o del Dirigente scolastico, profili sui vari Social Networks disponibili: l'eventuale apertura di pagine e profili sui social network richiede una specifica e formale autorizzazione da parte dell'Istituto Scolastico ed impone la redazione di specifiche procedure di utilizzo che ESCLUDANO il trattamento di qualunque dato
- è vietato utilizzare i profili eventualmente attivi per pubblicare dati personali di alunni, genitori, docenti, dipendenti o altri soggetti o per pubblicare video e filmati che li ritraggano
- l'apertura di profili personali sui Social Networks rientra nella sfera privata e non può assolutamente riguardare fatti, dati, notizie, immagini e video che riguardino l'attività professionale del soggetto:

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)

L'eventuale diffusione con tali strumenti di dati, immagini, video ecc. rientra nella responsabilità di chi, a TITOLO PERSONALE, utilizzi gli stessi provvedendone alla diffusione

- qualora l'apertura di un profilo scolastico ufficiale sia autorizzato dalla scuola, le credenziali per l'accesso devono rimanere nell'esclusiva disponibilità del Titolare del Trattamento che potrà inserire solo materiale non contenente dati personali o immagini o video o altre informazioni e notizie che possano ledere il diritto alla riservatezza dei soggetti
- l'utilizzo dei Social Networks da parte di soggetti esterni all'Istituzione Scolastica rientra nella facoltà/responsabilità degli stessi: ogni dato, immagine, video, notizia ecc. pubblicata da tali soggetti, esulando dal controllo del Titolare del Trattamento, non potrà certamente ascrivere a una responsabilità in tal senso dell'Istituto Scolastico: tuttavia è necessario far rispettare a tutti gli esterni il DIVIETO di effettuare foto o riprese video all'interno dell'Edificio Scolastico durante attività che non sono aperte al pubblico. Diversa la regolamentazione delle foto e video effettuati dai genitori in occasione di attività come gite, saggi ecc., che rientrano nella sfera privata e nella responsabilità, per l'eventuale successiva diffusione, dei soggetti che commettono il fatto
- è vietato creare gruppi whatsapp "di classe" per la comunicazione con i genitori degli alunni: per le comunicazioni Scuola-Famiglie è necessario utilizzare i canali ufficiali predisposti dall'Istituto Scolastico
- è vietato fornire direttamente ai Rappresentanti di Classe elenchi alunni e recapiti telefonici dei genitori: l'eventuale consegna di tali documenti costituisce grave violazione della normativa in materia di protezione dei dati personali
- è vietato inviare dati personali, foto, video o altre notizie tramite whatsapp ai genitori: tale invio costituisce grave violazione della normativa in materia di protezione dei dati personali
- per i gruppi whatsapp creati dai genitori valgono le stesse considerazioni fatte per i Social Networks

Per ogni dubbio in materia, prima di porre in essere qualunque comportamento che potrebbe essere lesivo, oltre che della riservatezza di terzi, anche della reputazione dell'Istituto Scolastico, rivolgersi al Titolare del Trattamento.

Utilizzo Piattaforme

L'utilizzo di Piattaforme e-learning come supporto all'attività didattica rappresenta sicuramente un valore aggiunto nell'erogazione del servizio di istruzione. Tuttavia è necessario adottare alcune cautele, soprattutto nel caso in cui per l'utilizzo di dette piattaforme sia richiesto l'inserimento di dati personali dell'alunno:

- redigere un ELENCO delle piattaforme che si intende utilizzare nello svolgimento dell'attività didattica: detto elenco dovrà essere comunicato al Titolare del Trattamento e dell'utilizzo di dette piattaforme dovranno essere informati i genitori degli alunni minorenni o gli alunni maggiorenni
- preferire l'utilizzo di piattaforme che non richiedano l'inserimento di dati personali degli alunni o consentano l'inserimento di dati ANONIMIZZATI
- di ogni piattaforma utilizzata è necessario verificare la nazionalità, in modo da escludere che si tratti di strumenti gestiti da soggetti residenti in Paesi Extra UE (rif. C.d. "Privacy Shield")
- prima di attivare l'utilizzo della piattaforma prendere visione delle MODALITA' DI UTILIZZO e della POLICY SULLA PRIVACY normalmente presente sul sito: è necessario verificare se i dati personali inseriti vengano trattenuti dal gestore della piattaforma
- l'elenco delle piattaforme da utilizzare dovrà essere reso disponibile, in occasione del primo incontro annuale con i genitori, agli stessi, in modo che possano prendere visione di tutte le informazioni previste

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)

- qualora sia necessario registrare l'alunno, tale registrazione dovrebbe essere effettuata direttamente dai genitori in modo da escludere eventuali contestazioni e da acquisire un consenso esplicito all'inserimento dei dati dell'alunno minore
- sulle piattaforme NON dovrebbero mai essere inserite foto, video, dati ecc. se non si è provveduto preventivamente alla ANONIMIZZAZIONE

Per ogni dubbio in materia, prima di porre in essere qualunque comportamento che potrebbe essere lesivo, oltre che della riservatezza di terzi, anche della reputazione dell'Istituto Scolastico, rivolgersi al Titolare del Trattamento.

Linee guida per la costruzione di parole-chiave

Al fine di costruire passwords sicure, considerato che sono molto rari i sistemi informativi che possono utilizzare parole chiave dinamiche, che vengono usate una volta sola, è indispensabile che ogni incaricato prenda buona nota delle modalità con cui è possibile selezionare parole chiave di difficile individuazione.

Parole chiave deboli

Le parole chiave di facile individuazione hanno le seguenti caratteristiche:

- La parola chiave contiene meno di 8 caratteri, anche se il sistema può accettare parole chiave di 8 caratteri ed oltre
- La parola chiave si può trovare in una comune dizionario italiano, in inglese od altra lingua comune
- La parola chiave è una parola di uso comune, come ad esempio il nome di qualche membro della famiglia, di animali da salotto, di amici, di collaboratori o di caratteri di fantasia.
- Sono da ritenere insoddisfacenti anche parole chiave legate a espressioni informatiche, hardware e software, come pure quelle legate a date di nascita od altre informazioni personali, come l'indirizzo, il numero telefonico e simili.
- Sono inoltre da scartare parole o sequenze numeriche del tipo aaaaaaa, bbbb, 121212, 123456, eccetera. Sono da scartare parole come sopra, digitate alla rovescia
- E' da scartare una qualsiasi delle parole chiave precedentemente indicata come debole, preceduta o seguita da una cifra come ad esempio giovanni1, oppure 1giovanni

Parole chiave sicure

Per contro, sono da ritenere parole chiave di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- Sono composte da caratteri maiuscoli e minuscoli
- Utilizzano anche caratteri di interpunzione, come; [,] , * " , ed una miscela di numeri e lettere
- Devono avere una lunghezza minima di 8 caratteri alfanumerici, se il sistema consente raggiungere questa lunghezza
- Non devono rappresentare una parola in una qualsiasi lingua o dialetto sufficientemente diffuso
- Non devono essere basate su informazioni personali, come nomi di membri della famiglia e simili
- Un altro importante accorgimento riguarda la selezione di parole chiave, che possano essere facilmente digitate sulla tastiera, senza doverla guardare, per ridurre al minimo il tempo di digitazione ed evitare che la digitazione possa essere osservata surrettiziamente da terzi nelle vicinanze

Le parole sicure non devono mai essere scritte o archiviate in linea.

- ✓ Ecco qualche indicazione per creare delle parole chiave sicure ma facili da ricordare:
- ✓ un primo suggerimento è quello di creare una parola chiave basata sul titolo di una canzone o su un'altra frase;

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)

- ✓ La parola chiave può essere formata abbreviando una intera frase come ad esempio "che gelida manina" diventa "chegemani"

Ecco alcuni altri esempi:

Frases	Possibile password
57% di Finlandesi hanno detto si alla EU	57%DFNHDSAEU
Roma è la capitale d'Italia	RMCPUEST
La mia macchia costa 27 milioni	MOPL27KKL
Meglio un uovo oggi che una gallina domani	MGLO/GLND
To be or not to be	(2B)V(12B)
Nel 1970 ho traslocato a Roma	I70I->RM
"Esc" si trova in alto a sinistra	"E"stULK
Gnu è un acronimo ricorsivo	GstACRR
Tutto è bene quel che finisce bene	2TBCFNB

ATTENZIONE!!!

NON USARE MAI ALCUNO DEGLI ESEMPI SOPRA ILLUSTRATI COME PAROLA CHIAVE

Raccomandazione per la protezione della parola chiave

Non utilizzare la stessa parola chiave per sistemi di autenticazione interni all'azienda e per sistemi di autenticazione esterni, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività, non legate all'attività aziendale.

Ove ad un incaricato vengano attribuiti diversi profili di autorizzazione, non deve essere usata la stessa parola chiave in relazione a differenti profili (ad esempio, deve essere scelta una parola chiave per l'accesso all'area tecnica del sistema, ed una parola chiave separata per l'accesso alla contabilità)

La parola chiave prescelta non deve essere condivisa con alcun soggetto, interno o esterno all'azienda, ivi inclusi i superiori, a qualsiasi livello.

Tutte le parole chiavi che sono state generate da un incaricato devono essere trattate come informazione strettamente riservata

In particolare, ecco un elenco delle cose che non bisogna fare:

- Non rivelate una parola chiave attraverso il telefono a chicchessia
- Non scrivete una parola chiave in un messaggio di posta elettronica
- Non rivelate la parola chiave al vostro superiore
- Non parlate di parole chiave di fronte di terzi
- Non date alcuna indicazione in merito al formato ed alla lunghezza della parola chiave, che utilizzate
- Non svelate la parola chiave su questionari o su formulari di sicurezza
- Non rivelate la parola chiave a membri della famiglia
- Non rivelate la parola chiave ad un vostro collega di lavoro, mentre voi siete in vacanza

Se qualcuno insiste per conoscere la vostra parola chiave, dapprima fate riferimento a questo documento e successivamente informate immediatamente il responsabile della sicurezza logica o il vostro titolare o responsabile

Non utilizzare mai la caratteristica, offerta da apparecchi ed applicazioni, di ricordare la parola chiave

Non scrivete la parola chiave su un qualsiasi documento e non nascondetelo in alcuna parte del vostro ufficio

Non archiviate la parola chiave in un qualsiasi tipo di sistema di elaborazione, incluso un telefono cellulare, un computer palmare e simile, senza utilizzare un algoritmo di cifratura.

Ricordatevi di cambiare la parola chiave almeno una volta ogni tre mesi.

Se avete anche solo il minimo sospetto che la vostra parola chiave sia stata in qualche modo compromessa o venuta a conoscenza di terzi, provvedete immediatamente alla sostituzione della parola chiave e riferite l'accaduto al responsabile della sicurezza logica, oppure al titolare od al responsabile del trattamento di dati personali.

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)

Si faccia attenzione che, nell'ambito delle misure di controllo del livello di sicurezza del sistema informativo, è possibile che il responsabile della sicurezza logica effettui tentativi di violazione della vostra parola chiave. Nel caso il tentativo abbia esito positivo, vi verrà chiesto di sostituire immediatamente la parola chiave.

Comunicazioni tramite posta elettronica

Ogni comunicazione elettronica riguardate gli interessati per finalità istituzionali devono essere effettuate utilizzando esclusivamente gli indirizzi di posta elettronica dell'istituto scolastico, previa verifica di correttezza dell'indirizzo del destinatario e seguendo le indicazioni del titolare

Informare immediatamente il titolare qualora si venga a conoscenza di circostanze idonee e determinare pericolo di dispersione o utilizzazione non autorizzata dei dati

Informare il titolare di ogni istanza di accesso al trattamento dati da parte degli interessati

Non fornire telefonicamente, verbalmente, via mail, per iscritto o con altro mezzo informazioni

Per trattamento dati sensibili e giudiziari attenersi alle disposizioni del REGOLAMENTO 305/2006

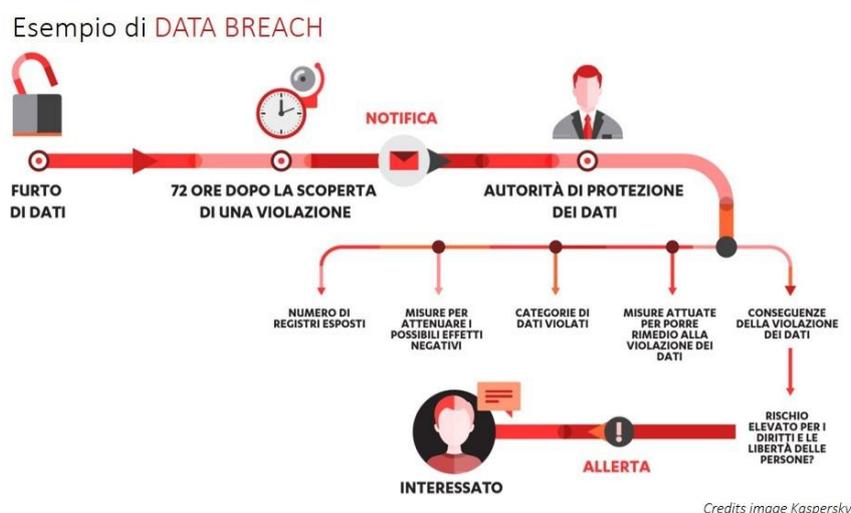
Violazione dei Dati Personali – PROCEDURA DI DATA BREACH

Una delle novità introdotte dal regolamento UE 2016/679 è la Procedura di Notifica al Garante di ogni violazione di dati (perdita, furto, distruzione ecc.) e che viene schematizzata nella seguente immagine

La procedura dettagliata è contenuta in uno specifico documento, che verrà distribuito alle funzioni direttamente coinvolte.

Ogni docente è tenuto a **comunicare tempestivamente** ogni violazione o sospetto di violazione dei dati personali facendone comunicazione al Titolare del Trattamento.

Sarà cura del Titolare procedere all'attivazione della relativa procedura.



Credits image Kaspersky

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
SAN NICANDRO GARGANICO (FG)

Richiesta di esercizio dei DIRITTI da parte dei soggetti interessati

Il Regolamento UE 2016/679 ha confermato alcuni diritti esercitabili da parte dell'Interessato, che vengono schematizzati nella seguente immagine



Sul sito internet del Garante per la Protezione dei Dati Personali è disponibile un MODELLO per l'esercizio dei Diritti da parte degli interessati

(<https://www.garanteprivacy.it/documents/10160/0/MODELLO+esercizio+diritti+in+materia+di+protezione+dei+dati+personali>)

ed una scheda di sintesi, che si riporta di seguito, sull'esercizio di tali diritti

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019



IISS DE ROGATIS – FIORITTO
SAN NICANDRO GARGANICO – CAGNANO VARANO
 Via Marconi – Villaggio studentesco Dr. V. Zaccagnino
 SAN NICANDRO GARGANICO (FG)

Scheda di sintesi a mero scopo divulgativo. Per un quadro completo della materia, si rimanda alla legislazione in tema di protezione dei dati personali e ai provvedimenti dell'Autorità.



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Conosci i principali diritti previsti dal Regolamento (UE) 2016/679?

Il Regolamento (articoli 15-22) riconosce importanti diritti in materia di protezione dei dati personali, che possono essere esercitati rivolgendosi al titolare del trattamento (soggetto pubblico, impresa, associazione, partito, persona fisica, ecc.).



Accesso ai propri dati personali



Hai il diritto di sapere se è in corso un trattamento di dati personali che ti riguardano e - se confermato - di ottenere una copia di tali dati ed essere informato su: l'origine dei dati; i destinatari dei dati; le finalità del trattamento; l'esistenza di un processo decisionale automatizzato, compresa la profilazione; il periodo di conservazione dei dati; i diritti previsti dal Regolamento.

Rettifica, cancellazione, limitazione del trattamento, portabilità dei dati personali

Puoi chiedere - nei casi previsti dal Regolamento - che i dati personali a te riferiti siano rettificati o cancellati, o che ne venga limitato il trattamento. Puoi inoltre chiedere che i dati che tu hai fornito al titolare siano trasferiti ad un altro titolare («diritto alla portabilità»), nel caso in cui il trattamento si basi sul tuo consenso o su un contratto con te stipulato e venga effettuato con mezzi automatizzati.



Opposizione al trattamento

Puoi opporvi al trattamento dei tuoi dati personali per motivi connessi alla tua situazione particolare, da specificare nella richiesta; oppure senza necessità di motivare l'opposizione, quando i tuoi dati sono trattati per finalità di marketing diretto.

Come si esercitano questi diritti?

Puoi presentare, gratuitamente e senza particolari formalità (per esempio, tramite posta elettronica, posta raccomandata, ecc.), una richiesta di esercizio dei diritti al titolare del trattamento (sul sito www.garanteprivacy.it è disponibile un modulo facsimile). Il titolare del trattamento è tenuto entro **1 mese** a rispondere alla richiesta, o a comunicare un eventuale ritardo nella risposta in caso di richieste numerose e/o complesse (la proroga non può comunque superare i 2 mesi). Se la risposta non perviene nei tempi indicati o non la ritieni soddisfacente, puoi rivolgerti al Garante per la protezione dei dati personali, mediante un reclamo ai sensi dell'art. 77 del Regolamento, oppure all'autorità giudiziaria.



Scopri di più su: www.garanteprivacy.it/home/diritti

CODICE DOCUMENTO	DESCRIZIONE DOCUMENTO	INDICE DI REVISIONE	DATA DI REVISIONE
FGIS007003-GDPR-005/B	CODICE DI COMPORTAMENTO PER I LAVORATORI ADDETTI AL TRATTAMENTO DEI DATI PERSONALI (INCARICATI) DOCENTI	0	02/05/2019