IL NUOVO REGOLAMENTO GENERALE UE SULLA PROTEZIONE DEI DATI PERSONALI N. 679/2016

Rev. 1.1 Dlgs 101/2018

Decreti e regolamenti

- Pubblicazione nella Gazzetta Ufficiale dell'Unione Europea n. 119/2016: **4 Maggio 2016**.
- Entrata in vigore 679/2016: **25 Maggio 2016**.
- Applicabilità in tutti i Paesi della UE: **25 Maggio 2018**.
- **Viene abrogata** la direttiva europea 95/46/CE (regolamento generale sulla protezione dei dati)
- **19 settembre 2018**. È la data di entrata in vigore del **decreto 101/2018** che va a modificare il **d.lvo n. 196 del 2003**

Nuovo regolamento

- L'idea di base del GDPR è: ogni cittadino europeo deve essere avvisato sulla raccolta dei suoi dati personali, e deve dare la propria esplicita autorizzazione.
- Con il nuovo regolamento, nell'epoca dei social, e-commerce, web app, ecc. possiamo decidere cosa mostrare di noi e cosa tenere per noi, ma deve essere una nostra scelta e non diritto dei fornitori di servizi ai quali affidiamo i nostri dati abusarne magari per rivendere le nostre informazioni a società terze.
- ogni cittadino europeo con il GDPR ha il diritto di chiedere e ottenere la copia, la rimozione, la rettifica dei dati in possesso dell'azienda che gli ha fornito un servizio.
- In Europa oltre al libero scambio di prodotti e servizi serviva un regolamento che uniformasse le regole per lo scambio dei dati e che fornisse la possibilità di regolamentare lo strapotere dei giganti del web.
- La natura globale di Internet comporta che si debbano adattare alle nuove regole tutte le aziende che vendono prodotti e servizi in Europa , anche se la loro sede principale è all'estero.

GDPR

E le istituzioni scolastiche?

Tutelare i dati personali:

- degli alunni
- delle famiglie
- dei dipendente (Insegnanti, personale ATA)
- soggetti esterni (fornitori, professionisti, ecc.)

Le scuole, quindi, sia pubbliche che private, hanno l'obbligo di informare (tramite apposita informativa) gli interessati delle caratteristiche e modalità del trattamento dei loro dati.
E' altresì importante che le scuole verifichino i loro trattamenti controllando se i dati siano eccedenti rispetto alle finalità perseguite.

I contenuti dell'informativa

Gli articoli 13 e 14 del nuovo Regolamento Europeo 16/679 elencano con precisione quali contenuti vanno obbligatoriamente inclusi nell'informativa sul trattamento dei dati personali:

- Chi è il Titolare del **trattamento**
- Se nominato, i recapiti del **DPO**
- Quali sono i trattamenti effettuati e perché
- Qual è la **base giuridica** del trattamento
- Quali sono i **dati** raccolti
- Se il trattamento comporta operazioni automatizzate, come la **profilazione**
- Se i dati verranno comunicati a soggetti esterne (responsabili esterni)
- Per quanto tempo saranno conservati e **in che modo**
- Se i dati saranno **trasferiti** in altri Paesi e come
- Quali sono i **diritti** dell'interessato.

GDPR

Novità D.Lgs. 101/2018

(modifica D.Lgs. 196/2003)

il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione.

- Alcuni esempi di servizi fruibili dai 14 anni: Facebook, Twitter, WhatsApp, Instagram, Pinterest, Snapchat, Tiktok, ecc. Giochi multiplayer online: Fortnite, World of Warcraft, League of Legends, Clash of Clans, The Sims. Blog/Forum/Chat, modi popolari, per i giovani, per connettersi con altri che condividono i loro stessi particolari interessi di gioco.

- La recente legge 71 del 2017 ha previsto che i minori possano chiedere l'oscuramento o la rimozione di contenuti offensivi senza dover informare i propri genitori. La richiesta va inoltrata al gestore del sito o al titolare del trattamento, e, in seconda battuta (questa volta a mezzo dei genitori), al Garante, che interverrà in 48 ore.

Tutela della privacy del minore

- La pubblicazione di una fotografia online si inquadra pacificamente nel trattamento di dati personali e sensibili, e costituisce interferenza nella vita privata del minore. In tal senso occorre fare particolare attenzione nel pubblicare immagini di minori, anche se si tratta dei propri figli.
- L'attuale normativa prevede un generale principio di preminenza dell'interesse del minore, il quale comporta delle limitazioni nel trattamento dei dati personali anche da parte dei giornalisti, il cui trattamento normalmente è svincolato da limiti, questi ha l'obbligo di non pubblicare informazioni o immagini del minore se non nell'interesse oggettivo del minore stesso.

RPD - DPO

- Il **Data Protection Officer** (di seguito **DPO**) è una figura introdotta dal **GDPR** (Regolamento generale sulla protezione dei dati 2016/679), pubblicato sulla Gazzetta Ufficiale europea L. 119 del 4 maggio 2016.
- La norma prevede che tutti gli **enti pubblici** ed **alcune categorie di aziende private** nominino un soggetto qualificato che si occupi in maniera esclusiva della protezione dei dati personali, aggiornandosi sui rischi e le misure di sicurezza.

Principali compiti del DPO

- **attività di informazione e consulenza** al titolare e ai dipendenti che eseguono il trattamento, sugli obblighi derivanti dal regolamento e da altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati;
- **sorveglianza sull'osservanza** da parte del titolare del regolamento e delle altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati, compresa l'attribuzione delle responsabilità, sensibilizzazione e formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- **cooperare** con l'autorità di controllo**,** e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

GDPR

La scuola tratta i dati per finalità di interesse pubblico

- Il trattamento dei dati, anche a protezione speciale, è consentito per **motivi di interesse pubblico rilevante**.
- L'art. 2.bb sexies del Codice Privacy autorizza l'istituto scolastico a trattare i dati degli alunni senza consenso per: ***istruzione e formazione in ambito scolastico, professionale, superiore o universitario.***

Lo stesso significato diversi modi per scriverlo

- **GDPR**: *General Data Protection Regulation*
- **RGPD:** *Regolamento Generale Protezione Dati*
- **DPO:** *Data Protection Officer*
- **RPD:** *Responsabile protezione dati*
- **DATA CONTROLLER***: Titolare del trattamento*
- **DATA PROCESSOR***: Responsabile del trattamento*

Autorità Garante Privacy

Tra i diversi compiti del *Garante* (www.garanteprivacy.it) rientrano quelli di:

- controllare che i trattamenti siano effettuati nel rispetto delle norme di legge
- Attività di controllo preventivo
- ricevere ed esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati

Sanzione Glovo

Come si presenta un reclamo

CHE COS'E' IL RECLAMO E COME SI PRESENTA AL GARANTE

Il reclamo è lo strumento che consente all'interessato di rivolgersi al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia di protezione dei dati personali (art. 77 del **Regolamento (Ue) 2016/679** e artt. da 140-bis a 143 del **Codice** in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento) e di richiedere una verifica dell'Autorità.

Il reclamo può essere sottoscritto direttamente dall'interessato oppure, per suo conto, da un avvocato, un procuratore, un organismo, un'organizzazione o un'associazione senza scopo di lucro. In tali casi, è necessario conferire una procura da depositarsi presso il Garante assieme a tutta la documentazione utile ai fini della valutazione del reclamo presentato.

Il reclamante potrà far pervenire l'atto utilizzando la modalità ritenuta più opportuna, **consegnandolo a mano presso gli uffici del Garante** (all'indirizzo di seguito indicato) o mediante l'inoltro di:

a) **raccomandata A/R indirizzata a: Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 Roma**

b) **messaggio di posta elettronica certificata indirizzata a: protocollo@pec.gpdp.it**
(questo indirizzo è configurato per ricevere SOLO comunicazioni provenienti da posta elettronica certificata)

Il reclamo e l'eventuale procura dovranno essere sottoscritti con firma autenticata, ovvero con firma digitale, ovvero con firma autografa (in tale ultimo caso, al reclamo dovrà essere allegata copia di un documento di riconoscimento dell'interessato/a in corso di validità).

MODELLO DI RECLAMO*

- formato .docx

- formato .pdf

GDPR

Acquisizione dati Green pass

L'Autorità Garante per la protezione dei dati personali ha scritto al Ministero dell'istruzione affinché sensibilizzi le scuole sui rischi per la privacy derivanti da iniziative finalizzate all'acquisizione di informazioni sullo stato vaccinale degli studenti e dei rispettivi familiari.

- Agli istituti scolastici non è consentito conoscere lo stato vaccinale degli studenti del primo e secondo ciclo di istruzione, né a questi (a differenza degli universitari) è richiesto il possesso e l'esibizione della certificazione verde per accedere alle strutture scolastiche.
- Per quanto riguarda i familiari, le amministrazioni scolastiche non possono trattare informazioni relative all'avvenuta o meno vaccinazione, ma limitarsi a verificare, mediante il personale autorizzato, il mero possesso della certificazione verde all'ingresso dei locali scolastici.
- Il personale scolastico (ATA, insegnanti) non è tenuto a dare nessuna spiegazione sullo proprio stato vaccinale.

Problemi relativi al Green Pass

- deroga dall'indossare la mascherina nelle classi in cui tutti gli studenti abbiano completato il ciclo vaccinale o posseggano un certificato di guarigione in corso di validità
  - il Garante ha confermato piena collaborazione al Ministero dell'istruzione per individuare misure attuative che consentano di soddisfare le esigenze sanitarie di prevenzione epidemiologica e, allo stesso tempo, assicurino il rispetto della libertà di scelta individuale e il diritto alla protezione dei dati personali. L'Autorità ribadisce la necessità che vengano in ogni caso individuate modalità che non rendano identificabili gli studenti interessati, anche al fine di prevenire possibili effetti discriminatori per coloro che non possano o non intendano sottoporsi alla vaccinazione.
- Uscite didattiche
  - articolo 2 del D.L. 111/2021 prescrive a tutti i soggetti che intendano accedere a determinati mezzi di trasporto di munirsi della certificazione verde COVID-19 (pullman con conducente).
  - Solo in zona bianca. Se è prevista l'uscita dal comune o dalla regione, il passaggio potrà avvenire solo tra due zone bianche.
  - L'esibizione del GP per alunni di età superiore ai 12 anni è necessaria anche nel caso in cui lo richieda l'ingresso a musei, teatri, cinema, piscine, ecc.

GDPR

Definizione di trattamento

- L'articolo 4 del nuovo Regolamento generale definisce il **trattamento dei dati personali** come qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Cosa intendiamo per dati personali?

Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

- **DATI COMUNI**

  Nome, cognome, codice fiscale, indirizzo di casa, ecc.

- **DATI PARTICOLARI**

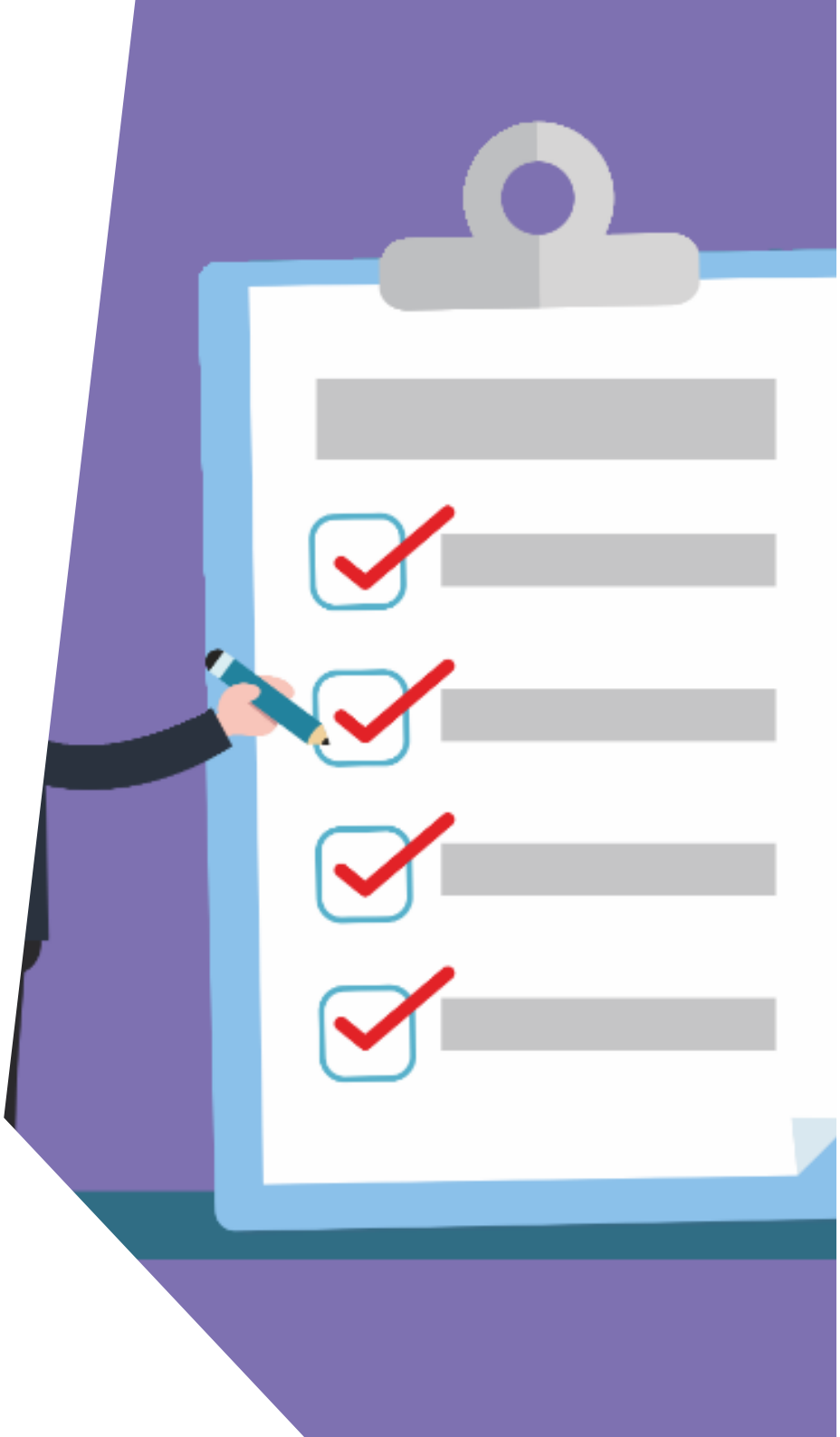
  dati che rivelino l'origine razziale o etnica, le opinioni politiche, condanne penali, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute (anche la semplice ferita ad una mano) o alla vita sessuale o all'orientamento sessuale della persona.

GDPR

Accountability

Il punto fondamentale del concetto di accountability è la dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità.

La responsabilità e l'obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance e di un buon modo di rispondere ai problemi che derivano dal trattamento dei dati. Solo quando si dimostra (ovvero si è in grado di rendicontare) "come" e "in che modo" si è provveduto a gestire quel problema il concetto di "responsabilizzazione" e della conseguente "Responsabilità" funziona effettivamente ed in concreto.



GDPR

Obblighi imposti alla scuola dal principio di responsabilizzazione

- *Fornire informazioni agli interessati in merito ai trattamenti*
- *Redigere un registro delle attività di trattamento*
- *Formare il personale*
- *Designare un responsabile della protezione dei dati*
- *Nominare i responsabili del trattamento dei dati e gli autorizzati*
- *Adottare opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato in base al rischio*
- *Notificare le violazioni dei dati alle autorità di controllo*

Chi sono gli attori?

- Titolare del trattamento
- Responsabile del trattamento
- Autorizzati al trattamento
- Responsabile protezione dati

Titolare del trattamento
(L'istituto nella persona del dirigente)

- Il **Titolare del trattamento** (*data controller*) è "*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*" (art. 4. par. 1, n. 7 GDPR). In sostanza il titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati.
- Il titolare del trattamento non è, quindi, chi gestisce i dati, ma **chi decide il motivo e le modalità del trattamento.**

Responsabile del trattamento

- l **responsabile del trattamento** (*data processor*) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR).
- Si tratta di un soggetto, **distinto dal titolare**, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.
- Il titolare del trattamento risponde della gestione effettuata dal responsabile, dovendo ricorrere a responsabili che presentino garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che soddisfino i requisiti del Regolamento (Considerando 81 GDPR), e che le sue decisioni siano conformi alle leggi.

Autorizzati al trattamento

(I dipendenti)

- Figura particolarmente importante nell'organigramma privacy è quella che nel Gdpr viene qualificata quale «persona autorizzata al trattamento dei dati personali» permanendo nella sostanza una identità di ruoli e modalità di nomina.
- L'autorizzato è colui che effettua materialmente le operazioni di trattamento sui dati personali. Può essere solo una persona fisica, e deve agire sotto la diretta autorità del titolare del trattamento.
- E' fondamentale tenere presente che in assenza della nomina di autorizzati, qualsiasi operazione svolta dai dipendenti o collaboratori del titolare non sarà qualificata come un utilizzo interno dei dati, bensì come una comunicazione a terzi, con le problematiche del caso (in particolare occorre un consenso specifico).
- l'attribuzione di compiti e funzioni inerenti il trattamento dei dati personali non implica l'attribuzione di compiti e funzioni ulteriori rispetto a quelli propri della qualifica rivestita ma conferisce soltanto il potere/dovere di svolgere i compiti le funzioni attribuite dal titolare;

GDPR

Didattica Digitale Integrata

Regolamento 679/2016

Rev. 1.1 Dlgs 101/2018

Il consenso

1) Le scuole sono tenute ad acquisire il consenso di alunni, genitori e insegnanti per attivare la didattica a distanza?

No. Gli istituti scolastici possono trattare i dati, anche relativi a categorie particolari[1] di insegnanti, alunni (anche minorenni), e genitori nell'ambito delle proprie finalità istituzionali e non devono chiedere agli interessati di prestare il consenso al trattamento dei propri dati, neanche in relazione alla didattica a distanza, attivata a seguito della sospensione delle attività formative delle scuole di ogni ordine e grado. Peraltro, il consenso di regola non costituisce una base giuridica idonea per il trattamento dei dati in ambito pubblico e nel contesto del rapporto di lavoro.

GDPR

Quando è richiesto

In sostanza, il consenso nel contesto scolastico è marginale e rilevante solo per attività facoltative e accessorie, come possono essere **comunicazioni promozionali o la diffusione di fotografie o video sul web.**

Insegnare a distanza

- Il docente, in qualità di soggetto autorizzato al trattamento dei dati, per conto dell'Istituto, si impegna a garantire, anche durante la sua attività di smart working il completo rispetto del regolamento in tema di trattamento dei dati
- L'autonomia del singolo docente nella scelta delle modalità di erogazione delle attività formative va esercitata nel rispetto della privacy ai sensi del regolamento GDPR
- Ogni utente - docente o studente - sarà responsabile dei contenuti trasmessi e delle modalità di utilizzo della piattaforma
- Il docente utilizzerà le piattaforme e gli strumenti connessi messi a disposizione dall'Istituto mediante il proprio device o quello fornito dall'Istituto

GDPR

Utilizzo della Webcam

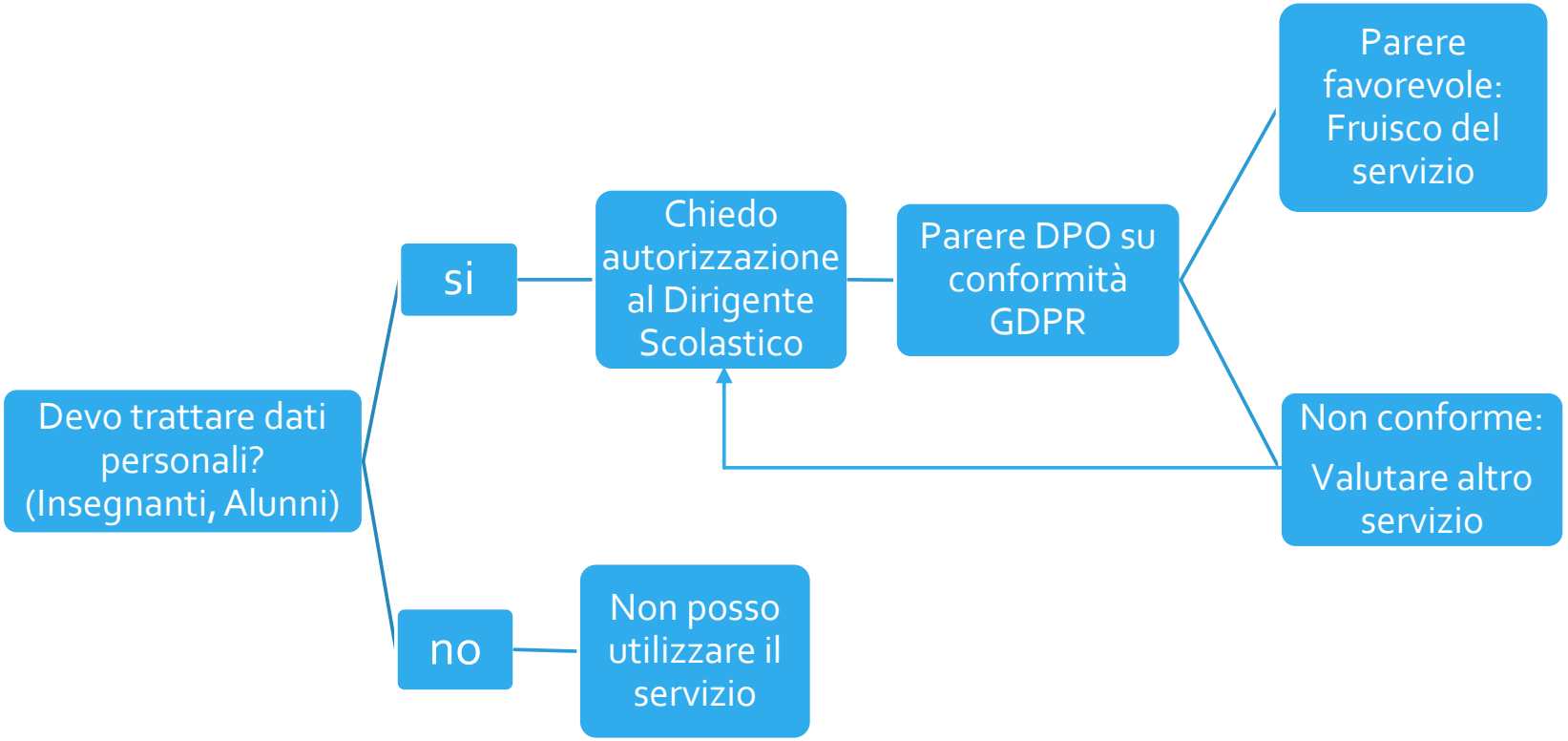
- Se l'alunno ha la webcam ma non vuole attivarla senza un giustificato motivo, allora di tale condotta negligente ne potrà tener conto l'insegnante ai fini dell'assegnazione del voto finale

- In assenza di un vero e proprio obbligo di attivare la webcam, il Ministero rivolge a entrambe le parti, docenti e studenti, l'invito a comportarsi diligentemente affinché la didattica a distanza possa funzionare.

- L'alunno non può essere obbligato ad usare la webcam se da tale impiego possa derivare un danno a un altro diritto, quale ad esempio quello alla privacy familiare: si pensi allo studente che abbia la disponibilità di un solo pc munito di webcam installato però nello studio privato del genitore, oppure in un luogo frequentato da tutta la famiglia, quale può essere la cucina, si pensi ancora allo studente che non voglia mostrare le pessime condizioni in cui versa l'immobile in cui vive.

Utilizzo di nuovi «strumenti»

comportamento insegnanti



Errori comuni

- Utilizzare strumenti non conformi per trattare dati relativi agli studenti (WhatsApp, email privata, Social, ecc.)
- Mandare email ad un gruppo di persone usando il campo «A» o «CC»
- Consegnare dati a enti, professionisti, aziende che lavorano per conto della scuola senza aver analizzato la possibilità di nominarli responsabili o autorizzati al trattamento
- Pubblicazione di foto e video di studenti e insegnanti sul sito web istituzionale senza aver acquisito il consenso informato
- Iniziare un trattamento senza pensare alle eventuali implicazioni che possono subentrare relativamente al trattamento di dati delle persone fisiche

FAQ Garante

GDPR

All'interno dell'Istituto servono delle regole, perché?

- I titolari del trattamento (dirigente scolastico), sotto la cui responsabilità ricadono abitualmente le problematiche di sicurezza, si trovano anche in virtù dei dettati della normativa privacy alla protezione delle informazioni custodite all'interno dei sistemi e a verificare di conseguenza il corretto utilizzo degli apparati in uso agli utenti finali (dipendenti, alunni).
- Si tratta di quelle misure adeguate definite nell'art. 32 del Regolamento U.E. 27 aprile 2016 n.679 anche se non meglio precisate sul piano tecnico.
- l'atteggiamento imprudente nell'uso di internet, di workstation e di smartphone può mettere a serio rischio tutta la struttura, con blocchi di produttività e, ora più che mai, di *data breach* ovverosia violazione di dati con tutti gli adempimenti che ne conseguono (art. 33 del medesimo sopraindicato Regolamento U.E.)

GDPR

Cos'è un data breach?

Con il termine data breach si intende un incidente di sicurezza in cui dati personali, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Solitamente il data breach si realizza con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a:

- **perdita accidentale:** ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati;
- **furto:** ad esempio, data breach causato da furto di un notebook contenente dati confidenziali;
- **infedeltà aziendale:** ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico;
- **accesso abusivo:** ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite

Come comunicare un data breach?

- Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del DPO.
- In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione compilando il modula A.

ALLEGATO A – MODULO DI COMUNICAZIONE DATA BREACH

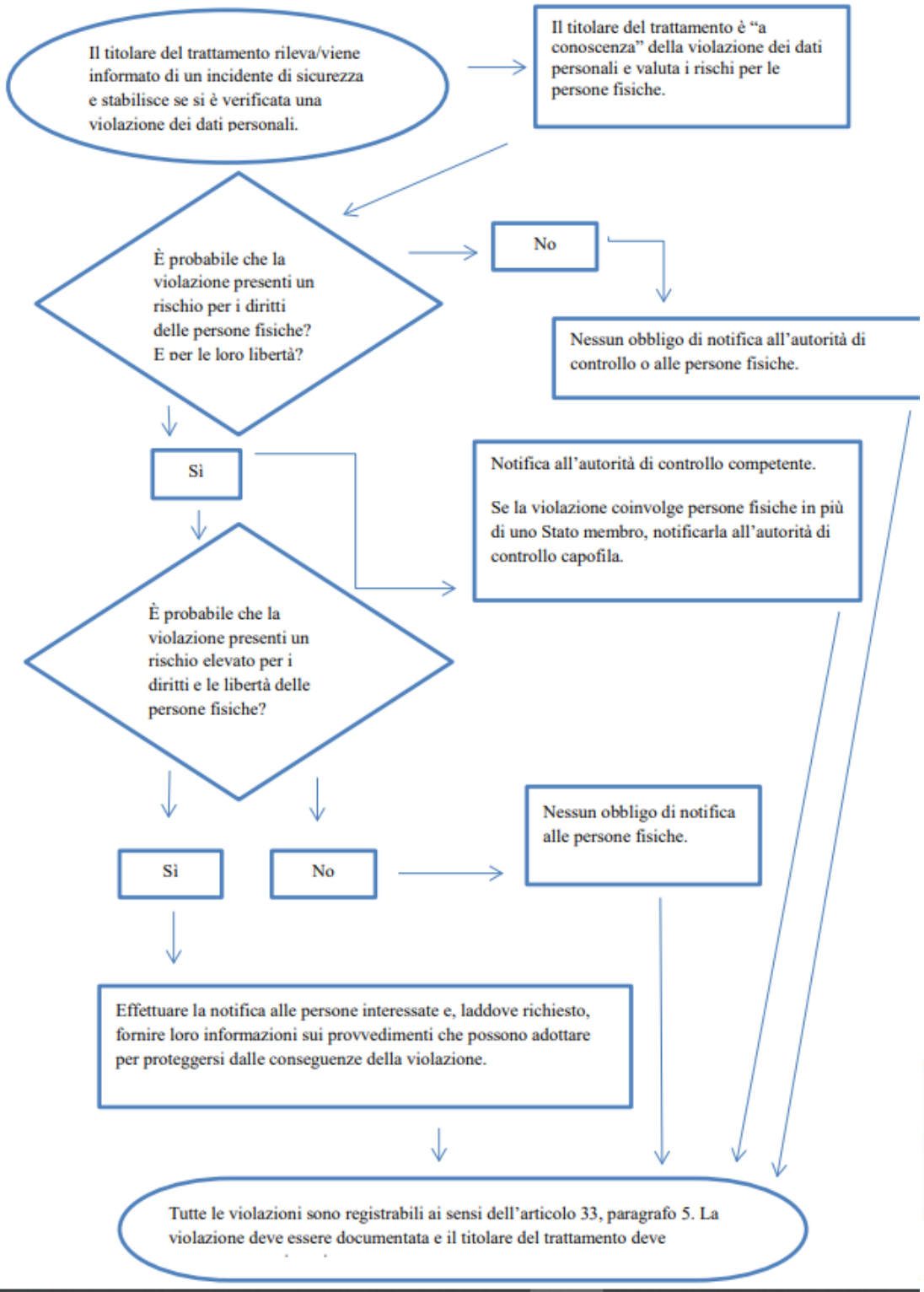
Qualora scopra un Data Breach, è pregato di compilare la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo:

.....

Comunicazione di Data Breach	Note
Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Nome della persona che ha riferito della violazione: Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico): in *caso di destinatario esterno indicare la ragione sociale:*	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione: Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	
Data creazione modulo:	

Quando notificare

A. Diagramma di flusso che illustra gli obblighi di notifica



Registro delle violazioni

Dettagli della Violazione					Conseguenze della Violazione	Interventi Intrapresi o da intraprendere			
Data	Natura dell'Evento	Descrizione della Violazione	Dati Interessati	Soggetti Coinvolti		Informativa Garante (SI/NO)	Informativa altri soggetti coinvolti (SI/NO)	Azioni Intraprese	Azioni da Intraprendere

- Natura dell'evento: Lettura informazioni sensibili, smarrimento chiavetta usb, distruzione involontaria documenti (verifiche, registri, ecc.)
- Dati interessati: nome, cognome, codice fiscale, dati relativi allo stato di salute, ecc.

Limitare i rischi
(più consapevolezza = meno rischi)

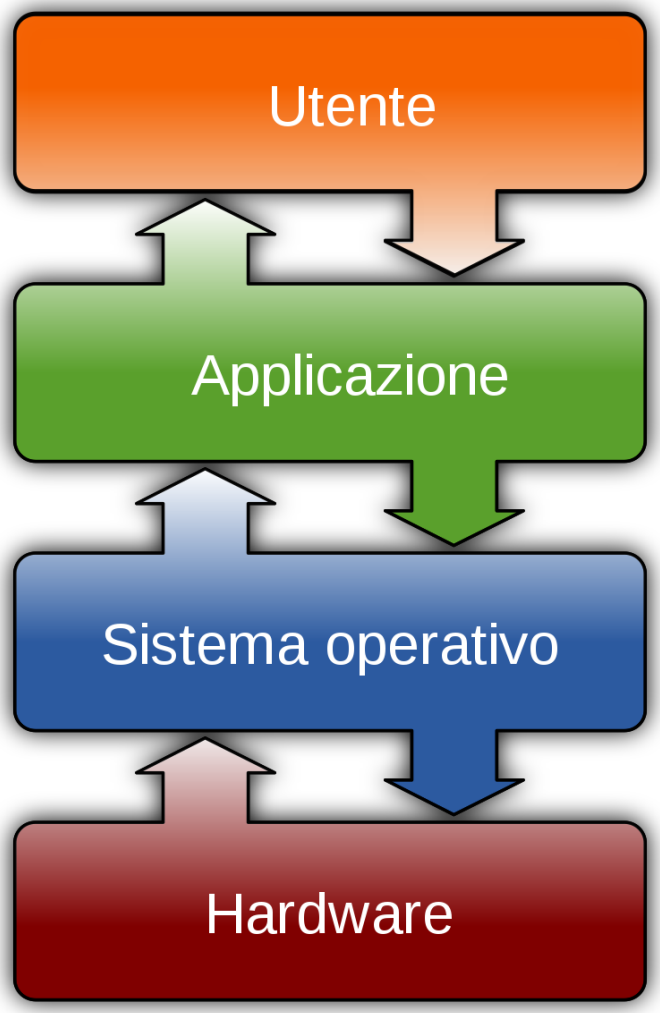
Spesso vengono ignorate le **minacce interne,** che sono dovute per lo più al fattore umano: ossia i comportamenti sbagliati degli stessi utilizzatori delle risorse informatiche a disposizione, dettati per lo più dalla mancanza di una cultura informatica di base. In questo senso, **lo scopo ultimo della formazione sulla sicurezza informatica deve essere quello di fornire le conoscenze minime** (magari anche qualcosa in più) per implementare quello che con una efficace espressione è definito il **firewall umano**. In sintesi, si tratta di fare in modo che gli utilizzatori siano in grado, al di là delle istruzioni che gli vengono impartite per svolgere le loro attività, di:

- riconoscere le **situazioni pericolose**;
- comportarsi correttamente al loro verificarsi;
- prevenirne gli effetti.

Cos’è un sistema operativo

Un sistema operativo (abbreviato in SO), in informatica, è un software di sistema che gestisce le risorse hardware e software della macchina, fornendo servizi di base ai software applicativi (programmi) installati.

Tra i sistemi operativi per computer troviamo Microsoft Windows, macOS, Linux.



Quali sistemi operativi sono compatibili con il GDPR?

GDPR

Quali sistemi operativi sono compatibili con il GDPR?

SISTEMI WINDOWS

Windows XP

non è più supportato dall'8 aprile 2014

Windows Vista

non è più supportato dall'11 aprile 2017

Windows 7

è supportato fino al 14 gennaio 2020

Windows 8.1

è supportato fino al 10 gennaio 2023 (utilizzo sconsigliato)

Windows 10

è supportato fino al 14 ottobre 2025

SISTEMI macOS

macOS Catalina

(10.15.6)

macOS Mojave

(10.14.6)

macOS High Sierra

(10.13.6)

macOS Sierra

(10.12.6)

GDPR

Le password

La password deve essere composta da almeno 8 caratteri, deve contenere almeno un carattere appartenente alle lettere maiuscole (da A a Z), deve contenere almeno un carattere appartenente ai primi 10 numeri di base (da 0 a 9), deve contenere almeno un carattere appartenente ai caratteri non alfabetici (ad esempio !,$,#,%)

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

Dove salvare le password?

Nel computer

non memorizzare mai le password nel browser (Explorer, Google Chrome, Mozilla Firefox…) perché chiunque acceda al tuo PC (ladri compresi) può facilmente accedere a tutti i tuoi ambiti privati e lavorativi.

Crea una lista di password attraverso excel, word o in qualsiasi altro programma che ti dia la possibilità di crittografare il contenuto del documento

Nel Cloud

Troverai molte soluzioni in internet (ad es. Passpack), quella che utilizzo io è Lastpass. Permette di creare le nuove password mentre navighi e le memorizza direttamente; tutti i siti sono poi accessibili solo con un'unica password. L'applicazione può essere scaricata in qualsiasi tuo PC o altro dispositivo.

Sulla carta

Scegli un piccolo quaderno o agenda, resistente perché non lo cambierai più, dove annotare le nuove password (metti anche il sito di riferimento, altrimenti non capisci più a che cosa si riferiscono). Tratta quel quaderno come il tuo portafoglio.

GDPR

Consigli utili per la sopravvivenza digitale

- Non utilizzare la stessa password per più servizi (email, siti, ecc.)
- Cambiare password almeno ogni 6 mesi
- Usare password sicure
- Controllare periodicamente questo sito: https://monitor.firefox.com/

La Crittografia

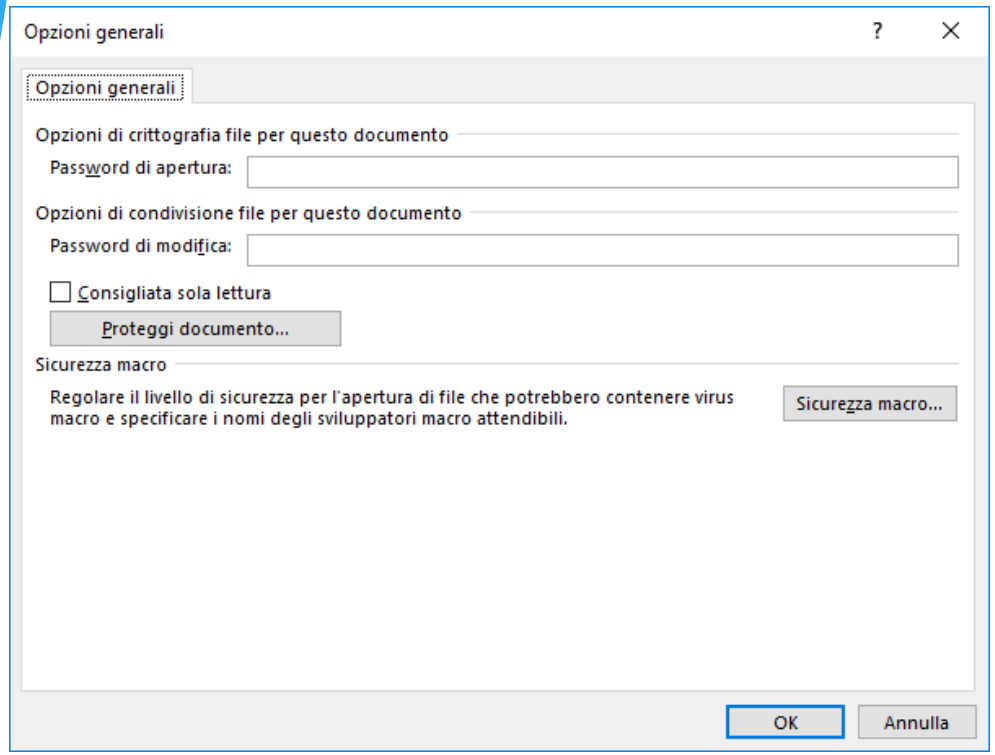
L'etimologia aiuta a capire: *Kryptós* (nascosto) e *graphía*(scrittura) sono le due parole greche che compongono il termine *crittografia*. Quest'ultima, infatti, altro non è che **un sistema pensato per rendere illeggibile un dato a chi non possiede la soluzione per decodificarlo**.

Quali file/periferiche posso crittografare facilmente:

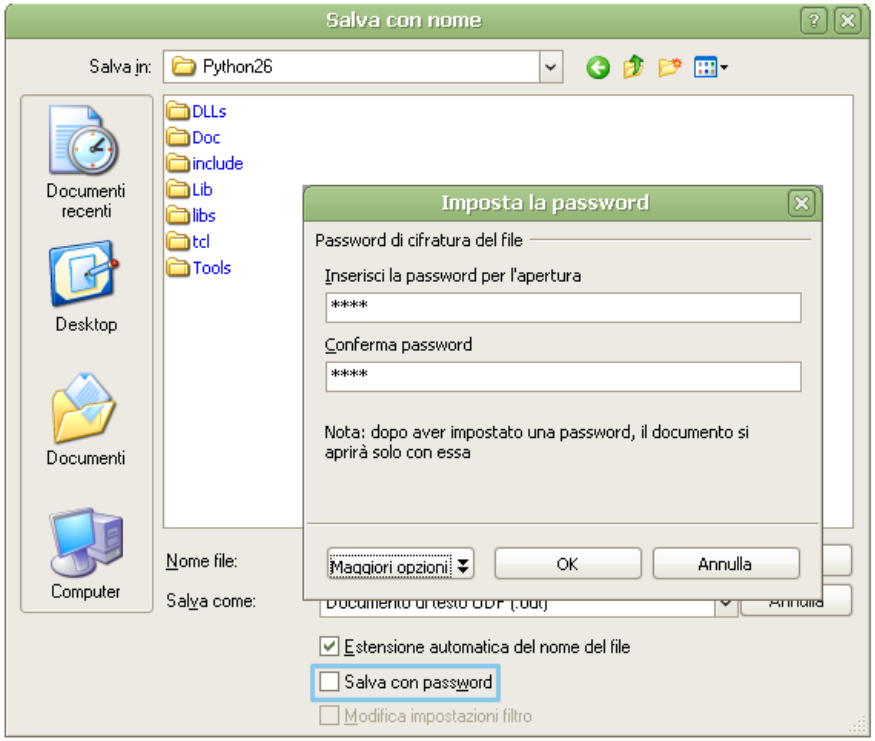
- Documenti (Word, Excel, Powerpoint, ecc.)
- File Zip (7zip)
- L'intero contenuto di chiavette usb (Bitlocker)

Crittografare i Documenti

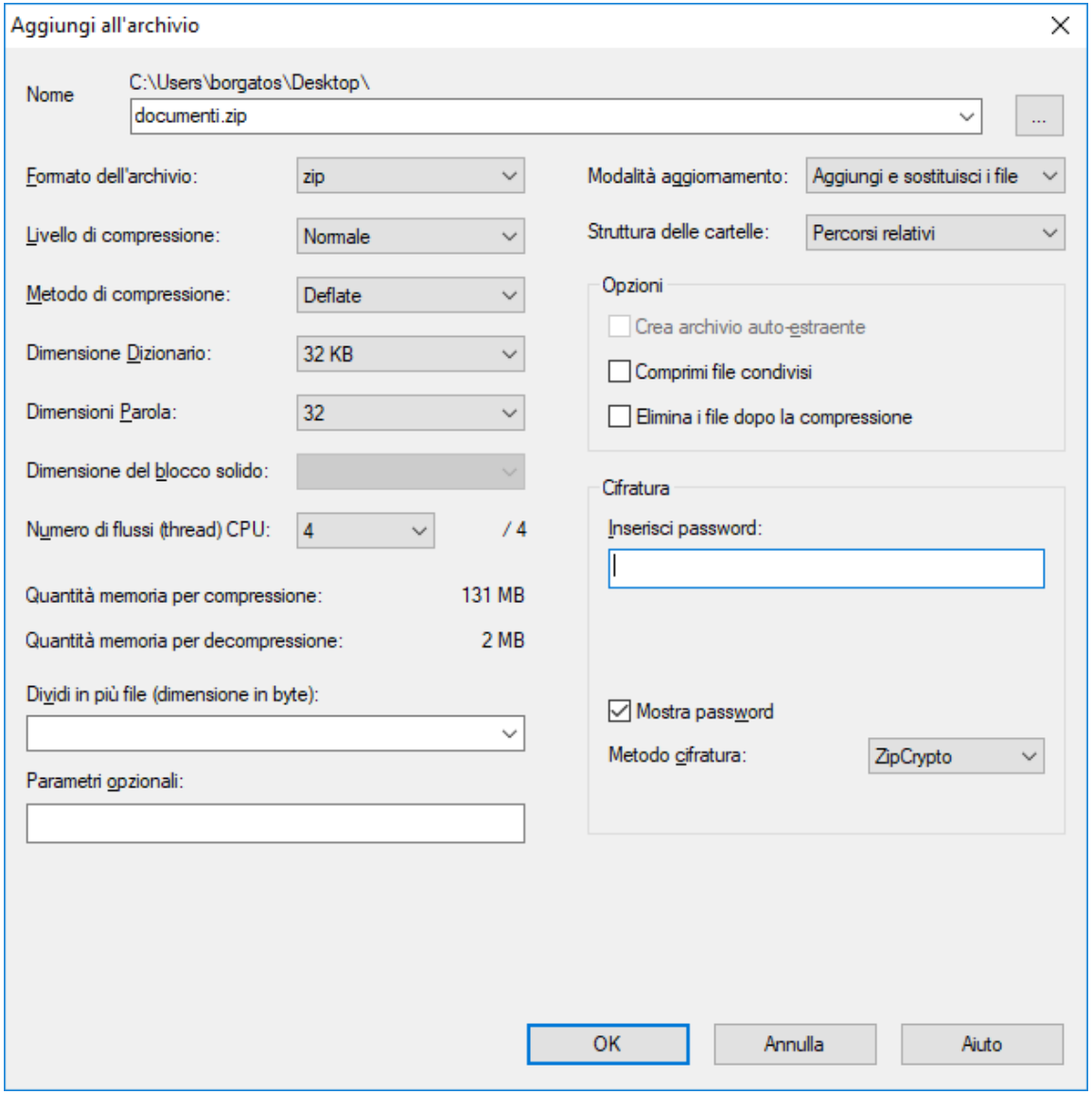
Word



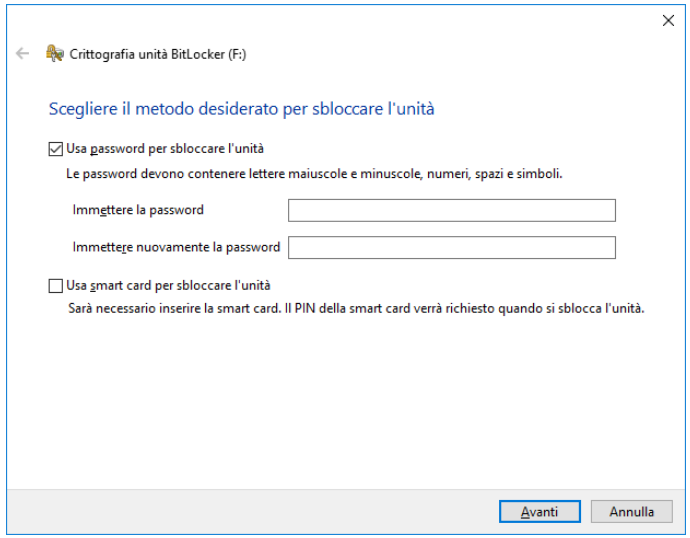
Open Office

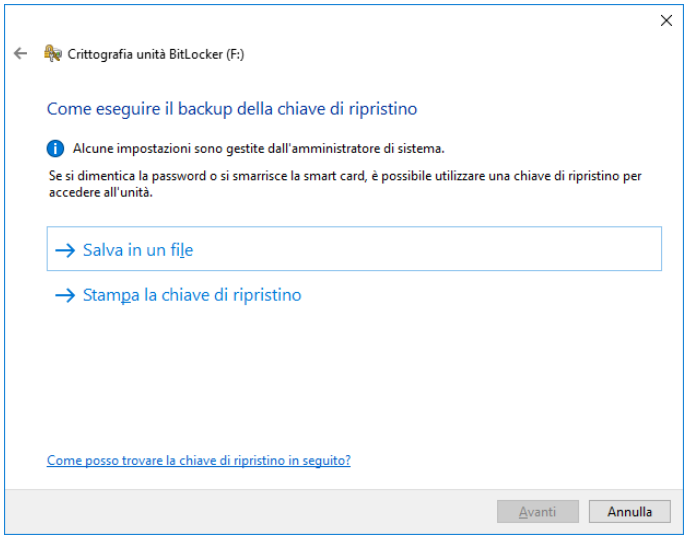


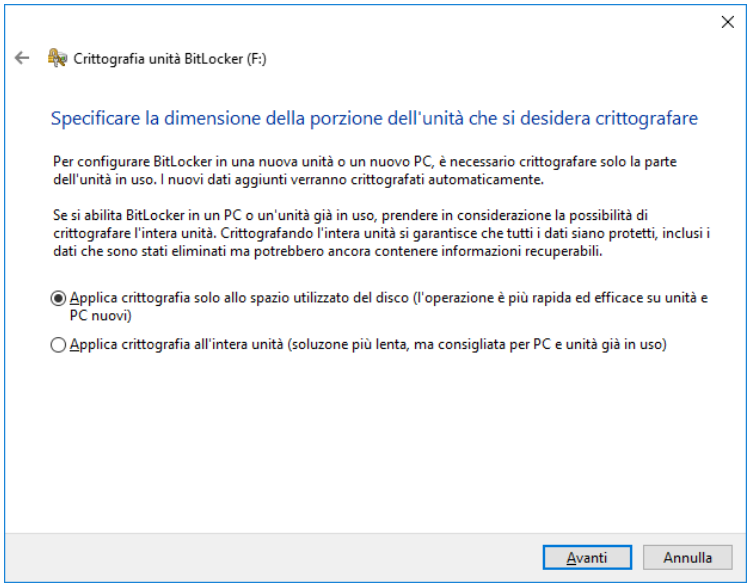
Crittografare File Zip

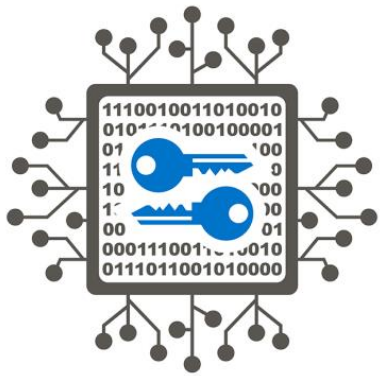


Crittografia dispositivo USB









GDPR

Capire se un sito è «attendibile»

- Una garanzia che un sito è sicuro è la presenza di un **Certificato SSL**, un certificato SSL (Secure Sockets Layer) è un protocollo standard che protegge le comunicazioni via Internet, in modo da assicurare che le informazioni sensibili fornite dagli utenti sul web (come password, dati personali e numeri di carte di credito) rimangano riservate e non siano in nessun modo intercettate da terze parti.
- Per fare ciò la comunicazione tra il client server e il server web è **criptata**. Per capire se navighiamo con una connessione che si basa su certificato/protocollo SSL basta **guardare l'indirizzo sulla barra di navigazione**. Nel nostro browser dove vedremo un **lucchetto** e anziché di **http://** troveremo **https://** sapremo che siamo su un sito che fa uso di certificati SSL. Questa garanzia protegge da frodi e furti, importante soprattutto se si ha a che fare con siti e-commerce e per tutti quei siti che erogano servizi online con scambio di dati delicati e privati.

GDPR

Capire se un sito è «attendibile»

- Sicuro
- Informazioni o Non sicuro
- Non sicuro o Pericoloso

Se si devono inserire dati sensibili, assicuratevi che sia presente il lucchetto verde e che il nome del certificato corrisponda al nome della pagina che stai visitando.

GDPR

Phishing

- Il **phishing** è un tipo di **truffa** effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.
- Si tratta di una attività illegale che sfrutta tecniche di ingegneria sociale: il malintenzionato effettua un invio massivo di messaggi di posta elettronica che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio. Per la maggior parte è una truffa perpetrata usando la posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS.
- Il phishing è una minaccia attuale, il rischio è ancora maggiore nei social media come Facebook, Twitter, ecc. Degli hacker potrebbero infatti creare un clone del sito e chiedere all'utente di inserire le sue informazioni personali. Gli hacker comunemente traggono vantaggio dal fatto che questi siti vengono utilizzati a casa, al lavoro e nei luoghi pubblici per ottenere le informazioni personali o aziendali.

GDPR

EN NE

Email «pericolose»

- I mittenti delle email di phishing sono (o meglio, sembrano essere) organizzazioni conosciute, come, appunto, banche o portali di servizi web, e hanno apparentemente uno scopo informativo: avvisano di problemi riscontrati con account personali dell'utente (home banking, portali di aste online, provider di posta elettronica, social network e altro) e forniscono suggerimenti su come risolvere le problematiche.
- Solitamente contengono messaggi allarmanti (del genere "Verifica il tuo account" oppure "Se non rispondi il tuo account sarà chiuso in 48 ore"), invitano a inserire informazioni personali e credenziali web in portali esterni.
- Le armi di difesa degli utenti contro questa forma di truffa informatica si basano tutte (o quasi) sul buon senso.
- Prima di tutto bisogna pensare che un'istituzione seria non chiederà mai i dati personali di un utente tramite e-mail.

GDPR

ENNE

Email «pericolose»

Nessuna grande azienda, o banca che sia, comunica con e-mail di servizi di terze parti ma solo con email che hanno come dominio l'indirizzo principale del loro sito web.

L'header è come l'intestazione che si trova su una busta che indica tutti i dati necessari al riconoscimento e infatti cercando in questa finestra troverete delle voci chiamate From , To e Replay To:

Email «pericolose»

GS

lunedì 11/02/2019 23:42

Galaxy S9 Plus <info@hartung.ru>

Hai Vinto un Galaxy S9 Plus ! 281979336

A Sergio Borgato

Criteri di conservazione Junk Email (30 giorni) Fine validità 13/03/2019

L'elemento scadrà tra 26 giorni. Per mantenere l'elemento più a lungo, applicare criteri di conservazione diversi.
I collegamenti e altre funzionalità all'interno del messaggio sono stati disabilitati. Per riattivare le funzionalità, spostare il messaggio nella cartella Posta in arrivo.
Il messaggio è stato contrassegnato come indesiderato tramite un filtro per la posta indesiderata diverso da quello di Outlook.
Il messaggio è stato convertito in formato di testo normale.

b7a37482c5f927a7

Gentile Cliente,

Ti informiamo che hai vinto un Galaxy S9 Plus, con la promozione "Galaxy Winter".

b7a37482c5f927a7

Per richedere il premio, e' necessario allegare un copia del tuo Documento D'Identita' a colori e in alta definizione (HD).

b7a37482c5f927a7

Allega subito una copia della tua Carta d identita fronte/retro a colori in alta risoluzione alla seguente email:

b7a37482c5f927a7

* Allega button: Carica Documento di identita <mailto:b7a37482c5f927a7@wintercold.info?Subject=Identita Samsung ID: borgato.sergio@enneuno.it>
* Allega manuale via mail: doc@wintercold.info

b7a37482c5f927a7

Una volta ricevuta tutta la tua documentazione ti contatteremo per la modalita' di invio dello Galaxy S9 Plus.

b7a37482c5f927a7

La promozione Galaxy Winter scade il 31.02.2019

b7a37482c5f927a7

Email «pericolose»

Prova a vincere gratuitamente un iPhone 11 Pro MAX.

Tim.it <nooreply@7TP.onehabiftchanges.com>
A [redacted]

In caso di problemi di visualizzazione del messaggio, fare clic qui per visualizzarlo in un Web browser.
Il messaggio contiene interruzioni di riga in eccesso.

TIM

SONDAGGIO CLIENTI 2020

Sei stato selezionato per ricevere un regalo esclusivo!

Per avere diritto a questa offerta speciale, tutto quello che devi fare è completare

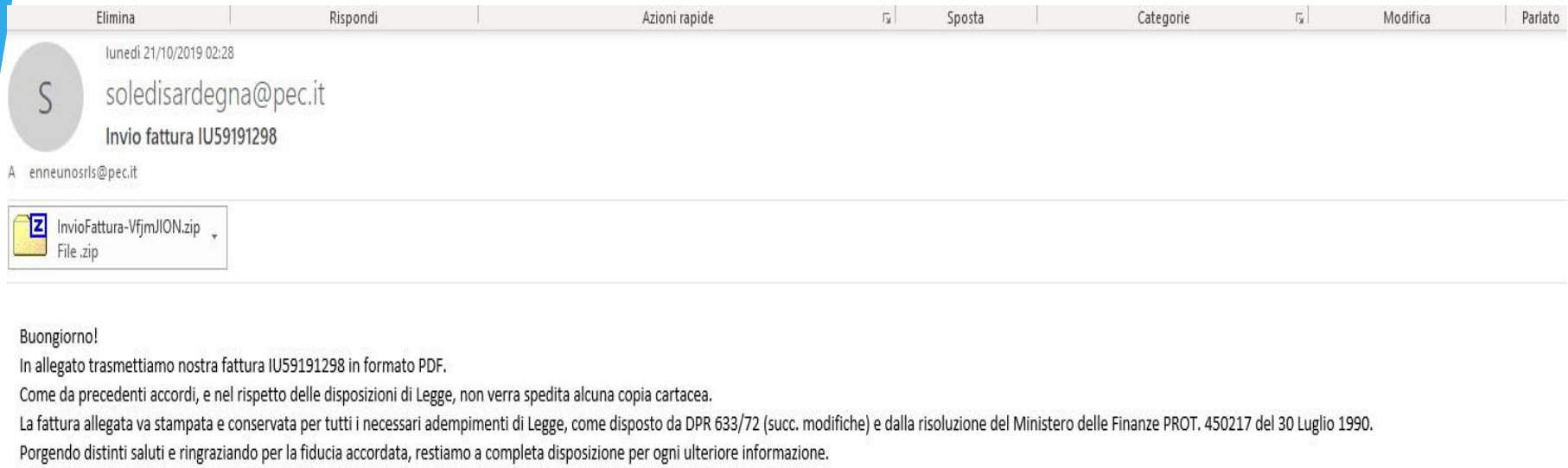
il nostro sondaggio di marketing. =>

- Vai alle Domande

Per fermarli, per favore vai
Qui o scrivi a:
o scrivi a: 801 US Highway 1
North Palm Beach, FL 33408

Se preferisci non ricevere ulteriori comunicazioni, annulla l'iscrizione Qui
Oppure scrivi a: PO Box 7775,,PMB 78292, San Francisco, California , 94120-7775

Email «pericolose»



Elimina | Rispondi | Azioni rapide | Sposta | Categorie | Modifica | Parlato

lunedì 21/10/2019 02:28

S

soledisardegna@pec.it

Invio fattura IU59191298

A enneunosrls@pec.it

InvioFattura-VfjmJION.zip
File .zip

Buongiorno!
In allegato trasmettiamo nostra fattura IU59191298 in formato PDF.
Come da precedenti accordi, e nel rispetto delle disposizioni di Legge, non verra spedita alcuna copia cartacea.
La fattura allegata va stampata e conservata per tutti i necessari adempimenti di Legge, come disposto da DPR 633/72 (succ. modifiche) e dalla risoluzione del Ministero delle Finanze PROT. 450217 del 30 Luglio 1990.
Porgendo distinti saluti e ringraziando per la fiducia accordata, restiamo a completa disposizione per ogni ulteriore informazione.

GDPR

EN NE

Email «pericolose»

martedì 12/02/2019 09:01

C

centroperativovvf@fastwebnet.it

AVVISO DI PAGAMENTO

A ⊞ **Info - N1 Servizi Informatici**

Criteri di conservazione Junk Email (30 giorni) Fine validità 14/03/2019

L'elemento scadrà tra 27 giorni. Per mantenere l'elemento più a lungo, applicare criteri di conservazione diversi.
I collegamenti e altre funzionalità all'interno del messaggio sono stati disabilitati. Per riattivare le funzionalità, spostare il messaggio nella cartella Posta in arrivo.
Il messaggio è stato contrassegnato come indesiderato tramite un filtro per la posta indesiderata diverso da quello di Outlook.
Il messaggio è stato convertito in formato di testo normale.

Buongiorno,

Invio nuovamente anche la fattura
Grazie e Buona Giornata

-- -- -- --

<https://docs.google.com/uc?export=download&id=0B2mfi20b5Sm1W12FA4P7bmZYTU0&revid=0B2mfi9jb5SmQNHo4NUgrdFJGaCt5bUp6SVJDMjYxVHT6XAL5YN>

Responsabile Amministrativa

GDPR

Portale Ticket e soluzioni
www.aiutoremoto.net

Modalità di assistenza

E' possibile ottenere assistenza inviando un'e-mail a: supporto@enneuno.it
oppure aprendo un ticket direttamente on-line da questa pagina.
Attendete le istruzioni di un tecnico nel caso sia necessario collegarsi in remoto al vostro computer.

Nuovo ticket

In caso di necessità, è possibile aprire un nuovo ticket di assistenza cliccando sul tasto qui sotto.

Apri nuovo ticket

Accedi al portale

Cliccando sul bottone qui sotto puoi accedere al portale di gestione dei ticket di assistenza.

Accedi al portale

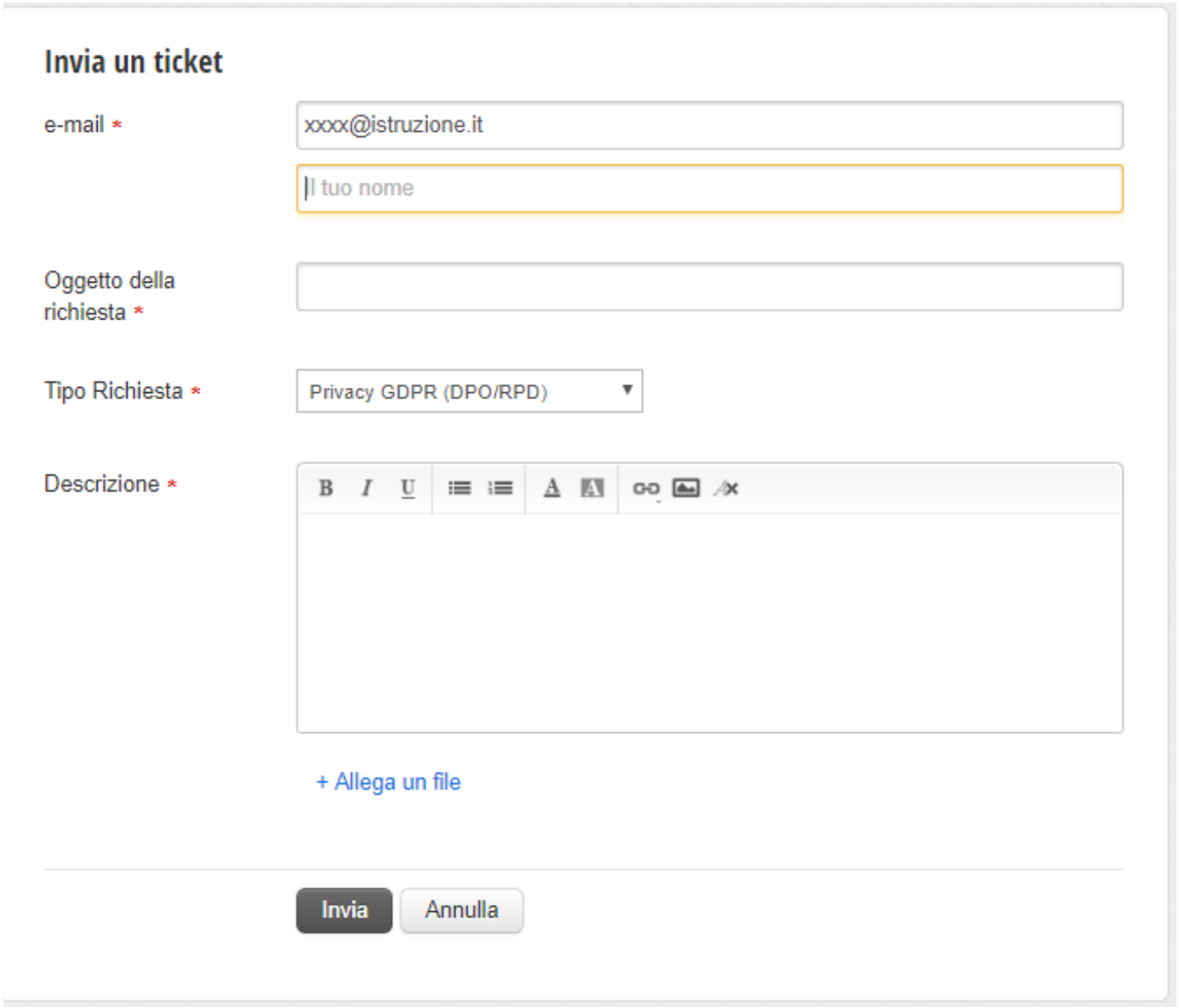
Controlla ticket

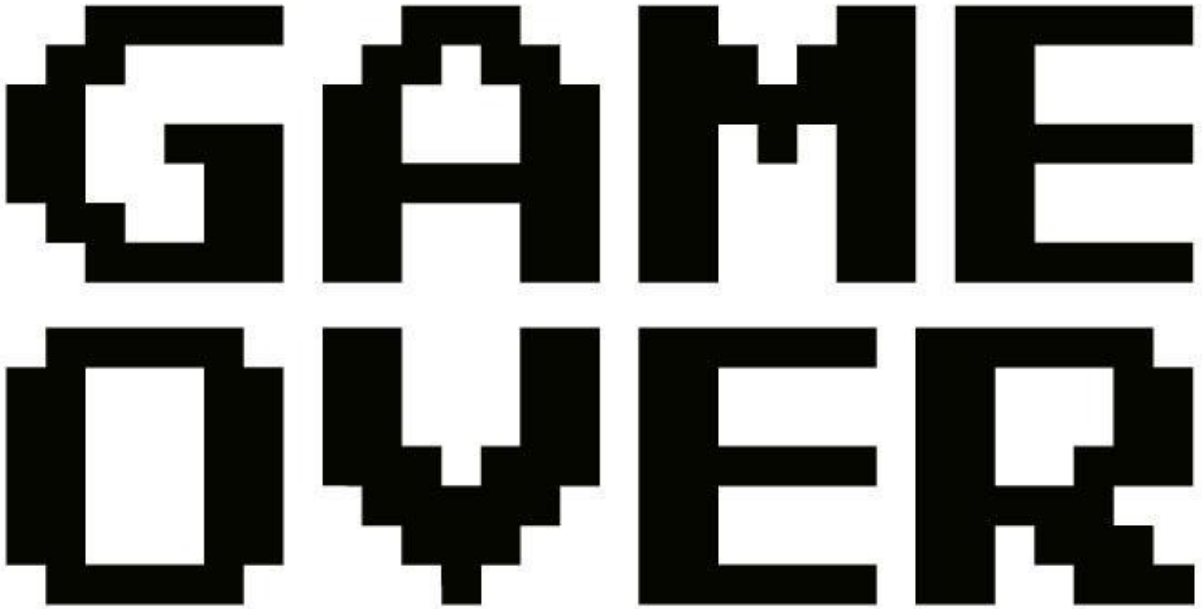
Controlla lo stato della tua assistenza cliccando sul tasto qui sotto.

Controlla ticket

GDPR

Portale Ticket e soluzioni





GDPR