



ISTITUTO STATALE DI ISTRUZIONE SUPERIORE  
**John Maynard KEYNES**

Via per Morazzone 37 – 21045 Gazzada Schianno (VA) - Tel. 0332-463213

Sito: <http://www.isiskeynes.edu.it> Mail: [vais01800p@istruzione.it](mailto:vais01800p@istruzione.it)

C.F. 95006130124

Pec: [isiskeynes@pec.it](mailto:isiskeynes@pec.it)



Mod. 1.1.0.3 Logo

**Prot:** (ved. segnatura)

DESTINATARI:

Tutti gli utenti dell'Ente

- **Personale ATA**
- **Personale Docente**
- **Collaboratori esterni**
- **Genitori**
- **Studenti**
- **Fornitori**

**Oggetto:** Nuova designazione del Responsabile della protezione dei dati e all'obbligo di notifica delle violazioni dei dati (cd. "**data breach**") – dott. Roberto DORIA della società Archè S.r.l..

Premesso che,

a far data dal 25 maggio 2018 è entrato definitivamente in vigore il **Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati)**, detto anche brevemente **GDPR**, da General Data Protection Regulation.

Trattandosi di Regolamento e non di Direttiva, il Regolamento è immediatamente esecutivo ed applicabile all'interno di ciascuno Stato, senza bisogno di alcun recepimento con atto normativo interno.

Tra le numerose e significative novità introdotte dal GDPR, vi è l'obbligo per tutte le Pubbliche Amministrazioni di designare, ai sensi dell'art. 37, il **Responsabile della protezione dei dati**, contraddistinto dall'acronimo **DPO**, da Data Protection Officer.

In ottemperanza a tale obbligo, l'Istituto ha inizialmente provveduto a designare il Responsabile della protezione dei dati nella persona del Dott. Giancarlo Favero, di Data Security ([www.datasecurity.it](http://www.datasecurity.it)), della ditta Swisstech S.r.l..

Tanto ciò premesso, con la presente circolare si

COMUNICA

che, in un'ottica di maggiore garanzia, efficienza ed economicità dell'azione amministrativa è stato ritenuto opportuno procedere alla sostituzione della figura in oggetto affidando l'incarico di **Responsabile della protezione dei dati (DPO)** alla cura del dott. **Roberto DORIA della società Archè S.r.l.** a decorrere dal 24 maggio 2019 (atto di nomina in prot. 3626 /2019 del 24/05/2019 e contestuale pubblicazione agli Albi).



Mod. 1.1.0.3 Logo

Tutti gli interessati (dipendenti, genitori, alunni, fornitori etc.) possono contattare il DPO all'indirizzo [segreteria@arche-va.it](mailto:segreteria@arche-va.it) oppure ai numeri telefonici (fisso) 0332 288036 e/o (mobile) 392-5680303, per porre qualsiasi quesito relativo alla normativa in materia di sicurezza e protezione dei dati, o relativo all'esercizio dei numerosi nuovi diritti dell'interessato introdotti dal GDPR.

In ottemperanza a quanto previsto dall'art. 37 comma 7 del GDPR, i dati di contatto del DPO sono stati comunicati al Garante per la protezione dei dati personali (<https://www.garanteprivacy.it/>) e saranno resi pubblici sul sito web istituzionale dell'Ente (<http://www.isiskeynes.it/>) in un'apposita sezione.

Come già rappresentato in occasione della precedente nomina del DPO si ripetono alcuni importanti concetti.

Una seconda significativa novità introdotta dal GDPR è l'**obbligo** per tutti i soggetti, sia pubblici che privati, di **notificare al Garante per la protezione dei dati personali, entro 72 ore, alcune tipologie di evento riconducibili alla fattispecie di "violazione dei dati personali"**.

E' pertanto necessario che tutto il personale sappia precisamente che cosa è una violazione dei dati personali, e le varie forme attraverso le quali tale evento può accadere. A tal fine si rammenta come il GDPR all'art. 4 (punto 12), fornisce la seguente definizione di violazione dei dati personali:

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

Da ciò deriva, contrariamente a quanto si potrebbe pensare, come la definizione di "violazione di dati personali" includa non solo le fattispecie in cui vi sia stato un accesso abusivo ai dati personali, ma anche il caso della distruzione o della perdita dei dati personali, eventi che si possono verificare con una certa frequenza, ad esempio a causa del guasto di un supporto di memorizzazione, di un virus informatico, di un non corretto svolgimento delle procedure di *backup*, etc. Altra importante casistica è quella di dati personali o sensibili comunicati o portati a conoscenza di soggetti, interni o esterni all'Istituto, non autorizzati o non titolari.

Tra le più probabili ipotesi di violazione dei dati personali in cui si può incorrere si annoverano:

- Furto o smarrimento di una chiavetta USB contenente dati personali
- furto di PC o tablet contenenti dati personali
- violazione del Registro elettronico
- smarrimento o furto di verifiche degli alunni
- inadeguata custodia dei dati vaccinali
- portare a conoscenza dati di un alunno al genitore per il quale sia stato emesso un Provvedimento



Mod. 1.1.0.3 Logo

da parte del Tribunale dei minori di revoca della potestà genitoriale

- soddisfare una richiesta di accesso agli atti, che comporti la violazione della privacy del c.d. "controinteressati"
- pubblicare dati personali eccedenti rispetto a quelli strettamente indispensabili per il raggiungimento delle finalità.

Tale elenco ha ovviamente carattere esemplificativo e non esaustivo.

È importante inoltre ricordare che la violazione dei dati personali non riguarda solamente i dati in formato elettronico, ma può riguardare anche i dati in formato cartaceo; questa seconda casistica, anzi, è la più critica da gestire, in quanto se vi fosse la perdita o il furto di fascicoli cartacei contenenti dati personali, tale evenienza potrebbe essere molto difficile da rilevare.

Si evidenzia a tal proposito quanto disciplina l'art. 33 del Regolamento UE 2016/679:

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

*2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.*

*3. La notifica di cui al paragrafo 1 deve almeno:*

*a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;*

*b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*

*c) descrivere le probabili conseguenze della violazione dei dati personali;*

*d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

*4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.*

*5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo."*



Mod. 1.1.0.3 Logo

In aggiunta, l'art. 34 del Regolamento UE 2016/679 prevede:

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

*2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).*

*3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:*

*a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;*

*b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;*

*c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analogo efficacia.*

*4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta."*

Si chiede, pertanto, di porre la massima attenzione nel monitorare e rilevare tempestivamente tutti gli eventi di tipo "violazione dei dati personali", **compresi gli eventi per i quali non vi sia la certezza ma anche solo un sospetto**, e comunicarli immediatamente al Dirigente Scolastico, il quale provvederà ad informare tempestivamente il DPO, che provvederà ad effettuare tutte le valutazioni del caso di concerto con il Dirigente Scolastico ed a predisporre, se ve ne siano i presupposti, la notificazione da effettuare entro 72 ore all'Autorità di Controllo nazionale (Garante per la protezione dei dati personali). Si ricorda che la tardiva od omessa notificazione al Garante di un evento di tipo "violazione dei dati personali" è punita con la **sanzione amministrativa pecuniaria fino a 10.000.000,00 di Euro**, ai sensi dell'art. 83 comma 4 lettera a) del Regolamento Europeo.

Il Dirigente Scolastico  
**Dott.ssa Fausa Zibetti**