Che cos'è il "GDPR 679/2016"

GDPR è l'acronimo inglese di "General Data Protection Regulation", ed indica il nuovo Regolamento Europeo sulla Privacy, entrato in vigore a livello di Comunità Europea il 24 maggio 2016.
Le norme sono applicate in tutti gli Stati membri dal 25 maggio 2018.

Il legislatore ha voluto introdurre regole più chiare in merito all'**informativa** ed al **consenso**, stabilendo precisi limiti al trattamento automatizzato dei dati; si è voluto rendere la norma più trasparente, con un'unica visione in tutta l'Unione Europea, rendendo molto chiara e semplice la gestione del proprio dato per ogni cittadino mediante consensi e revoche evidenti.

Le principali novità DEL REGOLAMENTO EUROPEO SULLA PRIVACY:

Cosa abbiamo fatto nel Vostro Istituto Scolastico:

- Identificato il **TITOLARE del TRATTAMENTO** che singolarmente determina le finalità e i mezzi del trattamento di dati personali, identificato nell'Istituto scolastico in persona del suo legale rappresentante ovvero del Dirigente Scolastico.
- Nominato il **DPO** (Data Protection Officer), figura di controllo e consulenza, priva di responsabilità esecutive, contattabile alla mail: info@privacycontrol.it oppure lombardia@privacycert.it.
- **Profilato** tutti i ruoli e funzioni per il trattamento dei dati (categorie dati, soggetti interessati, finalità, misure di sicurezza, ecc.)
- Nominato gli **incaricati del trattamento**, ovvero ognuno di voi, attraverso la nomina che avete già ricevuto
- Predisposto le **informative con i relativi consensi** conformi al GDPR:
  - Agli alunni/famiglie
  - Al personale (documento previsto nel contratto del MIUR)
  - su ognuno dei Vostri siti web (Fac simile solo da compilare e incollare nella pagina Privacy dedicata)
  - per tutti i fornitori (si ricorda che l'informativa "completa" deve essere inoltrata solo su esplicita richiesta, in quanto l'informativa breve è sempre inserita nei contratti firmati)
- definita la **DPIA** (Data Protection Impact Assessment), la Procedura di Valutazione di Impatto sulla Protezione dei Dati,
- completata l'analisi dei rischi e relative azioni correttive (**Allegato Misure di Sicurezza**)
- predisposto il **Registro dei Trattamenti**
- predisposte le **procedure** conformi al GDPR (Procedura Gestione esercizio dei diritti degli interessati tramite un modello fac-simile, Procedura Gestione Data Breach)
- Mappato il **sistema** e la **rete IT** al GDPR
- pubblicizzato i **canali di comunicazione** mail: lombardia@privacycert.it e info@privacycontrol.it per eventuali chiarimenti con il DPO.

In conclusione:

Il Dott. Massimo Zampetti, coadiuvato da tutto il Team di professionisti appartenenti a Privacy Control (*brand registrato di Privacycert Lombardia S.r.l.*), ha completato il progetto GDPR nei tempi e nei modi previsti dalla legge vigente; nei prossimi mesi verranno completate le azioni correttive contenute nel piano del trattamento.

Ora tocca a Voi:

L'Incaricato, cioè ognuno di voi, è tenuto a:

- **trattare** i Dati Personali esclusivamente per l'espletamento delle proprie mansioni e solamente durante l'orario di lavoro;
- **utilizzare** le sole informazioni necessarie per assolvere alle funzioni cui è preposto
- **trattare** i Dati Personali a norma di legge e secondo correttezza e conservarli in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- ove possibile, **verificare** che i Dati Personali siano esatti, integri, non modificabili, nonché disponibili;
- **accertarsi** che l'Istituto abbia messo a disposizione degli interessati l'Informativa Privacy;
- **consentire** l'esercizio dei diritti degli interessati;

- **collaborare** con gli altri Incaricati del medesimo trattamento, nel rispetto delle indicazioni ricevute;
- **avvertire** attraverso i canali di comunicazione (e-mail) sopra riportati il DPO, ovvero un referente Privacy per la gestione del Sistema Privacy dell'Istituto, qualora si verifichi un anomalo funzionamento del proprio dispositivo informatico o in caso di incidenti relativi alla sicurezza dei Dati Personali;
- **modificare** sempre la password dopo il primo utilizzo e provvedere a sceglierne una nuova avendo cura che:
  - non sia riconducibile in alcuna maniera alla propria persona;
  - sia lunga almeno otto caratteri per i computer, ovvero, nel caso in cui lo strumento elettronico non lo permetta, la lunghezza sia pari al massimo dei caratteri consentito dal dispositivo in questione;
  - contenga almeno un carattere numerico e/o un carattere speciale (ad es.: @, *, #);
  - sia diversa da quella precedentemente fornita.
- **sostituire** la password ogni sei mesi e, nel caso in cui siano trattati dati sensibili (ai sensi dell'art. 9 del GDPR, "categorie particolari di dati personali"), ogni tre mesi, nonché al primo accesso successivo a quello di un soggetto terzo, espressamente autorizzato dall'Istituto;
- **custodire** con cura le credenziali di accesso agli strumenti elettronici utilizzati per l'espletamento dell'attività lavorativa (username e password);
- **osservare** tutte le misure di sicurezza, già in atto o successivamente disposte dall'Istituto, atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, o trattamento non consentito dei Dati Personali;
- **archiviare** negli armadi o nei propri cassetti da chiudere a chiave, al termine della giornata lavorativa e quando ci si allontana dalla propria postazione di lavoro, eventuali documenti cartacei contenenti Dati Personali;
- **spegnere** il dispositivo informatico al termine della giornata lavorativa e attivare sullo stesso lo screensaver quando ci si allontana dalla propria postazione di lavoro;
- **controllare** e custodire i documenti cartacei fino alla loro restituzione per evitare l'accesso da parte di persone prive di autorizzazione e restituirli al termine delle operazioni affidate;
- le cartelle o fascicoli personali di dipendenti, fornitori, alunni o famiglie devono essere tenuti in archivi/armadi chiusi possibilmente con una serratura; ogni sera tutte le cartelle devono essere riposte e chiuse a chiave e la chiave riposta in luogo sicuro;
- **mantenere** la massima riservatezza sui Dati Personali delle quali sia venuto a conoscenza nell'adempimento dello svolgimento delle Sue attività.

Fermo restando quanto sopra, si precisa che è espressamente vietato all'Incaricato, salvo espressa e preventiva autorizzazione del Titolare, di:

- **effettuare** trattamenti di Dati Personali che non rientrano nei Suoi compiti;
- **iniziare**, all'interno dell'Istituto, un nuovo trattamento di Dati Personali ovvero modificare un trattamento già in essere senza un'autorizzazione pregressa;
- **comunicare** o diffondere a terzi (inclusi altri dipendenti dell'Istituto), i Dati Personali di cui è venuto a conoscenza nello svolgimento della propria attività;
- **comunicare** a terzi le credenziali di autenticazione, salvo che nei casi di prolungata assenza dell'Incaricato o situazioni di emergenza o urgenza, per esclusive necessità di operatività o di sicurezza dell'Ente Pubblico;
- **creare** nuove banche dati ove conservare i Dati Personali;
- **sottrarre** supporti informatici e/o cartacei contenenti Dati Personali.

Bergamo, 25 luglio 2018

Buon lavoro a tutti

Dott. Massimo Zampetti
Amministratore Delegato