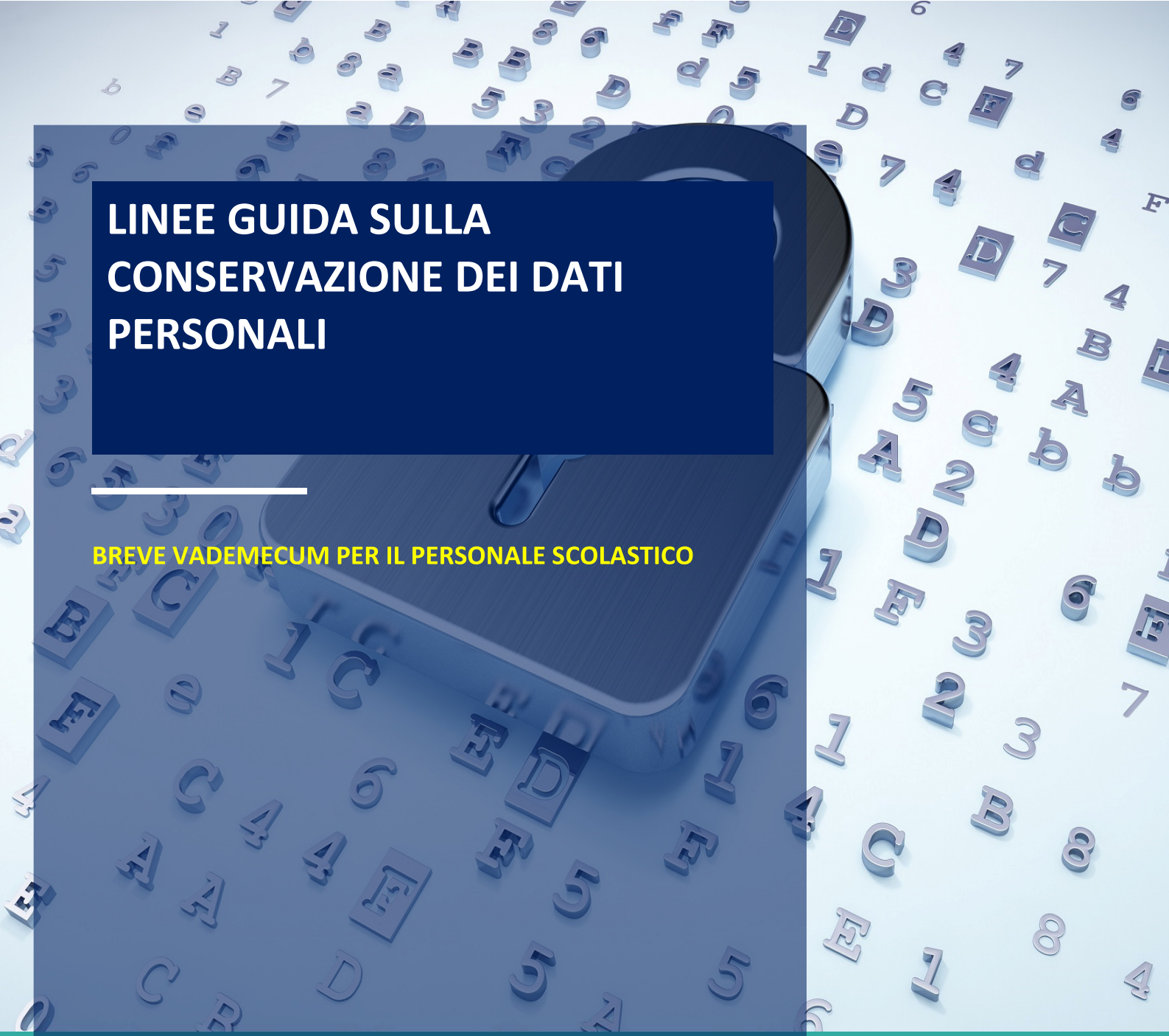

LINEE GUIDA SULLA CONSERVAZIONE DEI DATI PERSONALI

BREVE VADEMECUM PER IL PERSONALE SCOLASTICO

AUTORE: GEMINI CONSULT SRL © 2021

STUDIOPRIVACY

LINEE GUIDA SULLA CONSERVAZIONE DEI DATI PERSONALI

School survival guide

Queste linee guida sono state redatte per fornire alcune soluzioni '*de minima*' per la corretta gestione dei dati personali e per la conseguente tutela degli operatori scolastici. Il testo non può certo sostituirsi alla consapevolezza normativa che deve dimostrare di avere acquisito chiunque si trovi a dover gestire, a livello professionale, dati personali, ma può costituire tuttavia un aiuto, indicando le modalità con cui, in determinate situazioni, si devono trattare i dati personali.

La regola principale è che "non si devono conferire dati personali senza aver acquisito preventivamente le informazioni necessarie ad identificare il soggetto che ne fa richiesta"

- La prima cosa da considerare infatti è quella di capire se il nostro interlocutore ha titolo per poter richiedere determinate informazioni; pertanto la regola è che non si possono conferire dati personali a nessuno senza la necessaria preventiva identificazione dell'interlocutore, soprattutto quando la comunicazione avviene telefonicamente o via posta elettronica.

- La comunicazione dei dati personali interessa infatti tutti gli operatori scolastici, anche se in diversa misura: la segreteria scolastica, in funzione delle molteplici quotidiane richieste che pervengono negli uffici; i collaboratori scolastici quando rispondono al centralino; i docenti quando si relazionano fra di loro, o direttamente con gli studenti, e le relative famiglie, anche tramite applicazioni di messaggistica istantanea.

- Un altro aspetto da dover necessariamente considerare è che tutte le informazioni acquisite all'interno del contesto lavorativo sono soggette a riservatezza e, ove

previsto, al vincolo del segreto professionale ai sensi del Codice di Comportamento Nazionale (di cui al D.P.R. n. 62 del 16 aprile 2013). Pertanto si dovrà fare attenzione a come gestire determinate situazioni anche all'interno della scuola, valutando se il nostro interlocutore ha titolo per acquisire le informazioni, magari durante la pausa caffè.

Come dovrebbero essere gestite le attività della segreteria scolastica

Misure di sicurezza fisiche

- Non lasciare incustodito l'ufficio;
- Riservare la massima attenzione per i documenti che si trovano in locali accessibili al pubblico qualora contengano dati personali o informazioni riservate;
- L'accesso agli archivi (storici o in corso d'anno) deve essere consentito solo al personale espressamente autorizzato per iscritto in via permanente od occasionale;
- Gli archivi (storici o in corso d'anno) vanno mantenuti chiusi, compatibilmente con le esigenze di servizio, ed aperti solo quando è necessario;
- Le copie dei documenti che contengono dati personali o riservati vanno trattate con la medesima diligenza riservata agli originali;
- La riproduzione di documenti contenenti dati personali o riservati è vietata se non espressamente autorizzata dalla Direzione;
- Negli uffici l'ingresso deve essere consentito solo se non ci sono dati personali o informazioni riservate facilmente accessibili o quando non sono in corso telefonate che comportino il trattamento di dati personali o informazioni particolarmente riservate.
- Dopo l'orario di lavoro del personale dei singoli uffici di segreteria, tutti i dati sensibili e le informazioni riservate vanno conservate in arredi chiusi a chiave. Se non si possono chiudere gli arredi andrà chiuso ed interdetto l'Ufficio.

Misure di sicurezza tecnologiche

- Non lasciare incustodita la postazione tecnologica di lavoro o in disponibilità a terzi privi di titolo;
- Abilitare sempre l'oscuramento dello schermo del proprio computer, prevedendo la richiesta di inserimento della password di sistema al momento del ripristino della sessione di lavoro**;**
- Non disabilitare l'antivirus;

- Non installare software proveniente da fonti non ufficiali o comunque non autorizzato preventivamente dalla Direzione;
- Non lasciare le proprie credenziali relative ai computer/servizi/portali della scuola accessibili a terzi privi di titolo (post-it, appunti sul planning, file privi di protezione in cartelle condivise, agende o block notes);
- Effettuare sempre il log-out dai computer/servizi/portali utilizzati dopo che si è conclusa la sessione lavorativa;
- Evitare di utilizzare gli strumenti informatici della scuola per scopi personali (posta elettronica, social network, cloud privati, ecc.), onde evitare che tali attività, in alcuni casi facilmente hackerabili, possano compromettere, in tutto o in parte, il corretto funzionamento dei singoli dispositivi o dell'intera infrastruttura informatica della scuola, con tutte le responsabilità civili e penali che tali situazioni comportano a carico del dipendente.

Misure di sicurezza organizzative

Comunicazione di dati personali verso altri Titolari del trattamento (pubblici e privati):

Se il soggetto che richiede i dati personali è di diritto privato (esempio un'azienda, una cooperativa, un libero professionista, ecc.) il conferimento di dati personali è previsto solo se gli interessati hanno espresso il loro consenso. Di norma deve essere il soggetto esterno, in quanto Titolare autonomo, ad informare gli interessati ed a raccogliere il consenso. Tuttavia ci sono casi particolari, da valutare di volta in volta (comunicazione di dati personali per la gestione delle gite di istruzione, verso le strutture ricettive, comunicazione di dati personali per la certificazione delle competenze, ecc.), in cui può essere la scuola a richiedere il consenso direttamente agli interessati.

Se il soggetto che richiede i dati personali è di diritto pubblico (un'altra amministrazione pubblica quali il Comune, una ULSS, una Università, la Regione, ecc.) la comunicazione ha come presupposto necessario l'esistenza di una norma, di legge o regolamento. In assenza di una norma specifica, la scuola, prima di comunicare ad altre organizzazioni pubbliche i dati personali di cui è Titolare, dovrà informare l'Autorità Garante per la protezione dei dai personali e attendere un riscontro positivo, ovvero un silenzio di 45 giorni da considerarsi quale assenso, e ciò indipendentemente dalla necessità della comunicazione per lo svolgimento di compiti di interesse pubblico e di funzioni istituzionali.

Valutazione dei responsabili e gestione del Registro dei Trattamenti

Uno degli aspetti più delicati nella gestione della segreteria scolastica è la questione degli incarichi professionali a soggetti esterni, ove per soggetti esterni si intendono quei consulenti che, a vario titolo, necessitano di acquisire, in varia misura, dati personali in responsabilità della scuola per svolgere correttamente il loro incarico (RSPP, consulente Privacy, consulente informatico, fornitore del gestionale scolastico, ecc.). La normativa Privacy prevede espressamente che il Titolare (la scuola) valuti preventivamente il Responsabile (il consulente) che deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate per garantire la tutela degli interessati.
E' per questo motivo che il consulente, prima di essere contrattualizzato, deve dimostrare di avere i presupposti di cui sopra, onde evitare che il Titolare possa risultare passibile di pesanti sanzioni, nonché di eventuali richieste di risarcimento del danno da parte degli interessati stessi in caso di violazione dei dati personali. E' importante tenere presente inoltre che la valutazione del responsabile, nel caso di contratti pluriennali, andrà rinnovata con cadenza annuale. Infine è opportuno ricordare che la nomina di un nuovo Responsabile prevede necessariamente il contestuale aggiornamento del Registro dei Trattamenti in capo al Titolare.

Come dovrebbero essere gestite le attività dei collaboratori scolastici

Anche se i collaboratori scolastici accedono ad un numero limitato di informazioni, devono tenere comunque presente i presupposti citati all'inizio di questa guida. Inoltre bisogna fare attenzione a non lasciare incustodite dati personali o informazioni riservate al termine del proprio orario di lavoro (dati di primo soccorso, elenchi telefonici del personale e degli utenti, ecc.).
Un altro aspetto poi da dover necessariamente considerare è il controllo degli accessi alla scuola, che va monitorato anche grazie all'uso di specifici registri d'accesso; quando gli accessi, per motivi organizzativi, non sono costantemente presidiabili, questi vanno chiusi, in modo che i visitatori possano accedere ai locali della scuola solo in presenza del personale.

Come dovrebbero essere gestite le attività dei docenti

Misure di sicurezza organizzative
Uso dell'infrastruttura informatica della scuola:
Tranne nel caso in cui la scuola disponga di un'infrastruttura di rete interna particolarmente strutturata (server dedicati alla segreteria scolastica distinti dalla

didattica, servizi generalizzati di rete di Active Directory, antivirus e sistemi operativi aggiornabili, firewall e servizi di sicurezza dedicati a copertura di tutte le sedi della scuola, procedure generalizzate di backup su più livelli, ecc.), la conservazione di dati personali all'interno dei dispositivi informatici riservati all'uso didattico (sala insegnanti, laboratori informatici, computer collegati alle lim, ecc.) è sconsigliata, dato che potrebbero mancare tutti quei presupposti di sicurezza necessari alla tutela delle informazioni. In particolare è fondamentale che in area didattica non vengano conservati dati sensibili.

Misure di sicurezza tecnologiche

- Non disabilitare l'antivirus nei computer della didattica;
- Non memorizzare le credenziali che permettono l'accesso ai servizi/portali scolastici nei browser presenti nel dispositivo;
- Non installare software proveniente da fonti non ufficiali o comunque non autorizzato preventivamente dalla Direzione;
- Effettuare sempre il log-out dai computer/servizi/portali utilizzati dopo che si è conclusa la sessione lavorativa;
- Evitare di utilizzare gli strumenti informatici della scuola per scopi personali (posta elettronica, social network, cloud privati, ecc.), onde evitare che tali attività, in alcuni casi facilmente hackerabili, possano compromettere, in tutto o in parte, il corretto funzionamento dei singoli dispositivi o dell'intera infrastruttura informatica della scuola, con tutte le responsabilità civili e penali che tali situazioni comportano a carico del dipendente.

Uso dei device mobili (BYOD)

L'uso dei device mobili (personali/istituzionali in comodato d'uso) comporta l'adozione di alcune norme comportamentali a protezione dei dati. In particolare bisogna fare particolare attenzione a:

- Non lasciare incustodito lo strumento o in disponibilità a terzi privi di titolo;
- Proteggere il dispositivo con una password o un PIN di accesso. Non comunicare le credenziali d'accesso a terzi privi di titolo;
- Avere cura di conservare tutte le credenziali che permettono l'accesso al dispositivo e/o ai servizi/portali scolastici secondo la diligenza del buon padre di famiglia;
- Non memorizzare le credenziali che permettono l'accesso ai servizi/portali scolastici nei browser utilizzati;

- Abilitare lo screensaver o l'oscuramento dello schermo, e il conseguente nuovo accesso mediante inserimento delle credenziali;
- Abilitare adeguati strumenti di protezione: antivirus e, ove possibile, personal firewall, indipendentemente dal sistema operativo utilizzato dal dispositivo;
- Avere cura di condividere (posta elettronica, cloud) i documenti contenenti dati sensibili o riservati preferibilmente prevedendone la protezione tramite password di apertura o comunque con modalità che non ne permettano l'uso improprio da parte di terzi. Ove possibile utilizzare il registro elettronico per la gestione dei dati sensibili;
- Custodire nei dispositivi i dati sensibili o riservati preferibilmente prevedendone la protezione tramite password di apertura o comunque con modalità che non ne permettano l'uso improprio da parte di terzi, anche in caso di smarrimento o furto del dispositivo;
- Se si utilizzano i dispositivi a scuola, questi devono essere usati solo per scopi istituzionali, secondo le indicazioni del Regolamento d'Istituto sull'utilizzo degli strumenti informatici.
- Effettuare sempre il log-out dai servizi/portali utilizzati dopo che si è conclusa la sessione lavorativa (DAD, Registro Elettronico, ecc.).

Piattaforme per la Didattica a Distanza

Il presupposto per decidere se, e in che misura, utilizzare una qualsiasi piattaforma o app di terze parti a scuola, qualora preveda in particolar modo il conferimento di dati personali, è quello di dover, necessariamente e preventivamente, considerare quanto segue:

- I servizi Saas, Paas, Iaas, per poter essere utilizzati nella Pubblica Amministrazione, devono essere certificati dall'AGID (https://cloud.italia.it/marketplace/);
- Le scuole devono orientarsi verso strumenti che abbiano fin dalla progettazione e per impostazioni predefinite misure a protezione dei dati (Provvedimento Autorità Garante docweb 9302778/2020). Pertanto le piattaforme vanno valutate preventivamente, così come deve avvenire per i consulenti della scuola citati nel paragrafo dedicato alla segreteria scolastica. E' consigliabile quindi limitarsi all'uso di piattaforme che siano state, a vario titolo, consigliate a livello ministeriale (https://www.istruzione.it/coronavirus/didattica-a-distanza.html);

- Se la piattaforma prescelta comporta il trattamento di dati personali il rapporto con il fornitore dovrà essere regolato con contratto o altro atto giuridico (Provvedimento Autorità Garante docweb 9302778/2020);
- Le scuole dovranno assicurarsi che i dati trattati per loro conto siano utilizzati solo per la didattica a distanza (Provvedimento Autorità Garante docweb 9302778/2020).

Un altro aspetto da dover considerare è che le piattaforme per la didattica a distanza dovrebbero essere utilizzate solo ed esclusivamente conferendo i dati strettamente necessari alla corretta gestione del servizio (in pratica i soli dati identificativi – nome e cognome – degli utenti). E' fortemente sconsigliato quindi conservare in queste piattaforme dati eccedenti e soprattutto qualsiasi tipologia di dati sensibili.

Utilizzo di smartphone personali per lo svolgimento dell'attività professionale

Il ricorso a smartphone personali per la gestione delle varie attività scolastiche (realizzazione foto e video, utilizzo attivo di programmi di messaggistica istantanea, ecc.) può costituire un rischio. Non è infatti scontato che le applicazioni preinstallate dal fornitore del software, nonché quelle successivamente installate a titolo privato, siano in regola con il dettato della normativa Privacy, soprattutto se consideriamo che, quasi sempre, tali programmi richiedono, in varia misura, di poter gestire le telefonate e gli sms, l'accesso ai contatti ed alla galleria, ecc.. Attività queste che, se non correttamente valutate e gestite, fanno perdere il controllo sui dati personali e sulle informazioni conservate nel dispositivo, e che comportano, in caso di violazione, una possibile responsabilità a carico del dipendente.