Progetto Privacy
Privacy Officer Certificati

Anno Scolastico 2022/2023

RELAZIONE

del Responsabile Protezione Dati Personali

Titolare del trattamento

IC GASPARINI

Novi di Modena

Data: 02/5/2023

INTRODUZIONE

La scuola, in quanto ente pubblico, rientra nella casistica prevista dalla normativa per la nomina della figura del Responsabile della protezione dei dati (RPD), il quale deve essere nominato obbligatoriamente quando:

a) il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; oppure
b) le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Il Titolare ha quindi provveduto alla nomina di tale figura in Progetto Privacy Srl, referente Giampaolo Spaggiari, Privacy officer certificato TuV e Perfezionato in Data Protection e Data Governance presso l'università "La Statale" di Milano, i cui dati di contatto sono stati pubblicati sul sito internet del titolare.

Il presente documento è l'esito delle attività svolte dal RPD.

VERIFICHE E CONTROLLI SVOLTI

Le verifiche i controlli si inseriscono nella serie di obblighi in essere per la figura dell'RPD, quale organismo che deve assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento Europeo 2016/679 in materia di protezione dei dati personali di persone fisiche.

Durante l'incarico l'RPD ha informato la scuola circa gli aspetti generali del trattamento dei dati personali e sulle novità in merito e ha fornito supporto e consulenza su alcuni casi critici riportati dall'istituzione scolastica.

Le informazioni e il supporto sono stati forniti sia tramite contatti telefonici che e-mail, con incontri in presenza, online e attraverso webinar gratuiti su specifici argomenti.

Sono state inviate comunicazioni informative sui seguenti argomenti:

- Provvedimento Garante contro Google Analytics
- Monitora PA e Google Fonts
- Istruzioni privacy per inizio anno scolastico
- Check-list di controllo privacy 2022-2023
- Risposta ad accesso generalizzato MonitoraPA
- Compilazione griglia OiV per ANAC
- Obiettivi di accessibilità
- Parere su Nota di supporto MIUR Valutazione di conformità al GDPR del trattamento e trasferimento extra UE di dati personali degli utenti

Sono stati inoltre organizzati i seguenti Webinar gratuiti:

- Webinar Scuole Emergenza Covid
- Webinar accesso civico generalizzato MonitoraPA

Sono state svolte le seguenti attività:

- Incontro di verifica e controllo privacy con formazione degli incaricati presso la sede dell'istituto tenutosi in data 28/3/2023.

Sono state effettuate le verifiche sui trattamenti di dati personali posti in essere dal titolare verificandone la liceità e la attinenza alla funzione di istituzione scolastica. È stata verificata e valutata la documentazione privacy in possesso dell'istituto, l'organizzazione delle misure di protezione organizzative, logistiche ed informatiche, i trattamenti effettuati tramite internet, la presenza di apposite procedure per gestire eventuali violazioni di dati personali e di procedure volte a garantire agli interessati i loro diritti, la presenza di soggetti terzi debitamente autorizzati tramite accordi contrattuali che li individuano quali responsabili del trattamento ai sensi dell'art. 28 RGPD, la necessità di condurre una valutazione di impatto privacy.

STRUTTURA E ORGANIZZAZIONE DEL TITOLARE

La struttura organizzativa è composta dal titolare rappresentato dal Dirigente Scolastico, dalla Segreteria, dal corpo Docente e Collaboratori scolastici. Il Responsabile della Segreteria è il D.S.G.A., referente privacy interno per quanto concerne l'area contabile ed amministrativa.

All'interno della Segreteria i soggetti autorizzati al trattamento sono distribuiti nei vari uffici in base alle funzioni strumentali a loro assegnate.

L'elenco aggiornato dei soggetti autorizzati è reperibile presso la stessa Segreteria.

I soggetti esterni che trattano o possono accedere a dati personali sono stati individuati nei seguenti:

- ditte esterne che svolgono il servizio di assistenza informatica ai pc e reti presso il titolare. Questi soggetti vengono nominati amministratore di sistema tramite un accordo contrattuale di nomina a responsabile del trattamento;
- servizi di assistenza software e hosting relativi ad applicativi online utilizzati dalla Scuola per svolgere le ordinarie funzioni istituzionali. Su queste piattaforme vengono gestiti il registro elettronico e le funzioni relative alla "Segreteria digitale". Per queste funzioni i fornitori producono per loro stessi una nomina contrattuale a responsabile del trattamento, controfirmata dal titolare. In mancanza di questa, la Scuola deve proporre e raggiungere un accordo contrattuale di nomina a responsabile del trattamento;
- esperti esterni assunti per specifiche attività didattiche. Di norma questi soggetti (es. psicologo) svolgono attività come liberi professionisti non comunicando i dati alla scuola, operando così da titolari autonomi del trattamento. Vengono comunque individuati come soggetti autorizzati al trattamento nell'ambito del loro incarico;
- enti esterni i cui dipendenti e collaboratori svolgono funzioni di tutor o educatori degli alunni, venendo a contatto diretto con gli stessi. Questi enti vengono individuati quali responsabili del trattamento (art. 28 GDPR) e hanno l'obbligo di formare e informare i propri dipendenti circa i trattamenti da svolgere per la scuola.

Insieme ai referenti privacy del titolare sono stati analizzati i trattamenti di dati personali posti in essere dall'istituzione scolastica, valutando per ognuno di essi il rischio esistente per i diritti e le libertà delle persone fisiche.

L'istituzione scolastica gestisce e mette in atto trattamenti di dati personali di alunni e genitori, personale scolastico, esperti esterni e fornitori, il cui dettaglio è reperibile nel Registro delle attività di trattamento.

NORMATIVA PRIVACY APPLICABILE

Si è provveduto a verificare che tutti i trattamenti siano conformi alla normativa privacy vigente, al momento della stampa della presente relazione costituita da:

- Regolamento UE 2016/679 (RGPD)
- D. Lgs. 196/2003 Codice privacy modificato dal D. Lgs. 101/2018 Recepimento RGPD
- Provvedimenti del Garante

L'analisi è stata compiuta anche attraverso la condivisione di una check-list di controllo, strumento di lavoro con cui sia l'RPD che l'istituzione scolastica possono analizzare puntualmente e in dettaglio ogni aspetto del trattamento di dati personali della scuola.

EVIDENZE PRIVACY

Durante le verifiche sono emerse alcune evidenze relativamente a procedure e documentazione dell'istituto che risultano essere ancora non in linea con quanto prescritto dalla normativa vigente in materia di protezione dei dati personali.

In particolare, si prega di porre attenzione ai seguenti punti:

NON CONFORMITA' – DA RISOLVERE ENTRO 1 MESE DALLA NOTIFICA

Non presenti.

AZIONI CORRETTIVE – DA ATTUARE ENTRO 3 MESI DALLA NOTIFICA

Non presenti.

SUGGERIMENTI PER IL MIGLIORAMENTO – DA ATTUARE ENTRO 6 MESI DALLA NOTIFICA

1) Aggiornare la pagina Privacy del sito come indicato dal RPD

RACCOMANDAZIONI SU SPECIFICI TRATTAMENTI

Le raccomandazioni si riferiscono a trattamenti di dati personali che la scuola può mettere in atto e su cui occorre porre particolare attenzione.

GESTIONE DEI DATI PERSONALI ALUNNI BES/DSA/L.104 (DATI PARTICOLARI EX ART. 9 RGPD)

È indispensabile che questi dati, appartenenti a categorie particolari (stato di salute), siano protetti ed accessibili ai soli autorizzati. L'accesso a questi dati, in custodia della segreteria, deve avvenire solo quando sono presenti gli addetti della segreteria. Detto ciò, quando gli addetti sono assenti, i fascicoli vanno conservati in armadi chiusi a chiave.
L'utilizzo della chiavetta USB, non essendo dotata di autenticazione informatica se non cifrata, mette ad alto rischio i dati in essa contenuti che possono essere facilmente sottratti o acceduti da parte di soggetti non autorizzati. Si consiglia quindi di togliere i dati dalla chiavetta (formattandola) e di inserirli all'interno di una chiavetta dotata di cifratura oppure utilizzare un altro dispositivo ad accesso sicuro.

In caso di utilizzo di strumentazione informatica, è indispensabile che l'accesso di ogni utente alla piattaforma sia tracciabile e che si disponga di diversi livelli di autorizzazione. Sarà necessario creare dei gruppi di autorizzazione chiusi relativi a ogni

singola classe per la condivisione di dati particolari (DSA, BES, PEI) ed evitare così ulteriori diffusioni. In tal modo si evitano l'utilizzo di altri sistemi di comunicazione non tracciabili e non sicuri (e-mail). Si raccomanda che i files siano protetti da pseudonimizzazione o cifratura.

Si consiglia di comunicare ai genitori/tutori di far consegnare le certificazioni sempre e solo direttamente in segreteria, consegnandola in altri punti non viene assicurata la necessaria protezione, prevista dall'Art. 32 del RGPD, ai dati personali appartenenti a categorie particolari (Art. 9 RGPD). Qualora non fosse possibile fare altrimenti, occorre sensibilizzare chi riceve la documentazione circa la protezione e sicurezza dovuta a questo tipo di dati personali, suggerendo ad esempio di applicare delle tecniche di pseudonimizzazione, in modo da rendere i documenti temporaneamente anonimi tramite la sostituzione di nome e cognome con un codice o altro.

GESTIONE DEI DATI PERSONALI IN SEGRETERIA

Si suggerisce di conservare la documentazione contenente dati personali sempre in armadi chiusi a chiave con chiavi affidate ai soggetti autorizzati. Si raccomanda di non lasciare documenti abbandonati sulle scrivanie dove tutti possano prenderne visione. I documenti vanno conservati per il periodo di tempo necessario, stabilito dalle tempistiche dettate per le istituzioni scolastiche dal MIUR. Si consiglia di non gettare nel cestino dei rifiuti documenti cartacei se non siano stati prima resi illeggibili e si suggerisce di acquistare un distruggi documenti nel caso in cui non sia già disponibile.

I visitatori non devono poter prendere visione di dati personali direttamente dallo schermo dell'operatore. In questi casi, si consiglia di girare la postazione in modo da permettere all'addetto la custodia dei dati personali anche in presenza di visitatori all'interno dell'ufficio.

I dati contenuti nei fascicoli personali, appartenendo a categorie particolari di dati (c.d. sensibili), prevedono una maggior tutela da parte dei soggetti autorizzati al loro trattamento. Si consiglia di concentrare i fascicoli personali negli armadi chiudibili a chiave e di non permettere a personale non autorizzato di accedervi, sia durante che dopo l'orario di apertura della segreteria. Si consiglia di fare in modo che sia l'addetto della segreteria a consegnare il singolo fascicolo richiesto al docente e che la consultazione avvenga sotto il controllo degli addetti della segreteria in modo da evitare che i docenti possano accedere ai fascicoli di tutti gli alunni e non solo a quelli a loro autorizzati.

Si consiglia di tenere vuota la cartella temporanea scansioni, anche tramite la creazione di uno script (programma software) per l'eliminazione automatica periodica delle scansioni. I file scansionati devono essere subito spostati nelle cartelle del server di loro competenza.

CANCELLAZIONE DEI DATI PERSONALI DALLE PIATTAFORME ONLINE

Una volta uscito lo studente o il dipendente dalla scuola, non essendoci più le basi del trattamento in quanto l'interessato non è più nel perimetro gestionale dell'istituzione scolastica, non è possibile mantenere tali dati personali a disposizione della scuola, occorre quindi cancellare immediatamente gli account dalle piattaforme educative digitali all'uscita della persona e altri account presenti e intestati all'interessato (pc, registro elettronico, e-mail, ecc.).

FOTO E VIDEO CON IMMAGINI DEGLI STUDENTI

Si suggerisce in via preferenziale di richiedere un consenso specifico agli esercenti la responsabilità genitoriale per queste modalità particolare di trattamento dati dei minori.

Si consiglia di pubblicare solamente foto e video relativi ad eventi inseriti nel Piano dell'offerta Formativa dell'Istituzione Scolastica ove i genitori sono preventivamente informati della pubblicazione e di programmare anche un tempo massimo di pubblicazione oltre il quale verranno cancellati.

Nel caso in cui le foto degli studenti sono utilizzate per attività promozionali dell'Istituto, (es. open day) si raccomanda di raccogliere un consenso specifico degli stessi al trattamento delle loro immagini per un periodo oltre il normale percorso scolastico.

Si invita a non permettere la pubblicazione di commenti a foto e video pubblicati.

COPIE DI DOCUMENTI DI IDENTITÀ

L'utilizzo indebito delle copie dei documenti di identità può recare grave danno agli interessati. L'acquisizione e la conservazione della copia di un documento di identità va limitata il più possibile, adottando altre soluzioni quali ad esempio la registrazione dei soli estremi del documento. Qualora fosse indispensabile conservare la copia del documento di identità, occorre custodirlo in cassetti o armadi chiusi a chiave a cui possa accedere solo il personale autorizzato.

TRATTAMENTI SVOLTI IN ESTERNO DA ALTRI SOGGETTI

Particolare attenzione occorre dedicare ai trattamenti svolti all'esterno dell'Istituzione scolastica. La maggior parte degli adempimenti amministrativi e delle attività didattica vengono svolte oggigiorno tramite l'ausilio di portali online, forniti da ditte esterne private, a cui la Scuola affida i dati personali gestiti: con ognuno di questi soggetti deve essere presente un accordo contrattuale firmato per la nomina a responsabile esterno del trattamento, secondo quanto previsto dall'art. 28 del RGPD.

GESTIONE DEI DATI PERSONALI IN AMMINISTRAZIONE TRASPARENTE

Il Garante con provvedimento del 15 maggio 2014 in merito alla riutilizzabilità dei dati pubblicati ha ritenuto opportuno che i soggetti pubblici inseriscano nella sezione "Amministrazione trasparente" un alert generale sulle modalità di ripubblicazione. La dicitura va messa nella pagina principale di accesso all'Amministrazione trasparente nei seguenti termini: *"Si avvisa che i dati personali pubblicati in questa sezione sono riutilizzabili solo alle condizioni previste dalla normativa vigente sul riuso dei dati pubblici, in termini compatibili con gli scopi per i quali sono stati raccolti e registrati, e nel rispetto della normativa in materia di protezione dei dati personali."*

Il Garante con provvedimento del 28 maggio 2014 ha dettato le linee guida per osservare correttamente gli obblighi di trasparenza e privacy nelle pubblicazioni online di dati personali. Invitandovi a prenderne visione, ricordiamo qui alcuni punti del documento. Per quanto riguarda i dipendenti pubblici, non si possono riprodurre sul web i dati sullo stato di salute, i cedolini dello stipendio, l'orario di entrata e di uscita, l'indirizzo privato, la e-mail personale. Sono invece conoscibili da chiunque i livelli retributivi, i tassi di assenza, i risultati raggiunti, l'ammontare dei premi collegati alle performance, ma solo se in forma anonima o aggregata. Possono essere diffusi la retribuzione e i curricula di dirigenti, segretari comunali e provinciali, gli incarichi di collaborazione e consulenza, il ruolo dei dirigenti, i ruoli di anzianità e i bollettini ufficiali. Beneficiari di contributi economici e agevolazioni: è possibile pubblicare l'albo dei soggetti cui sono stati erogati contributi, sovvenzioni, crediti, o riconosciute agevolazioni, sussidi o altri benefici. In tali elenchi possono essere riportati i dati

identificativi (nome, cognome e data di nascita) omettendo invece di indicare il codice fiscale, le coordinate bancarie, le informazioni che descrivano le condizioni di indigenza e le informazioni sullo stato di salute.

Non risulta necessario rendere pubblici i dati personali dell'esperto esterno (indirizzo e-mail personale, telefono, residenza), che consigliamo quindi di togliere dal CV pubblicato online e da tabelle pubblicate in amministrazione trasparente.

GESTIONE DEI DATI PERSONALI NELLE COMUNICAZIONI ALLE AZIENDE (LICEI E ISTITUTI SUPERIORI)

È possibile provvedere a comunicare o diffondere "anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali" degli studenti e altri dati personali, diversi da quelli rientranti nelle categorie particolari di dati di cui all'art. 9 del Regolamento UE 2016/679. Ciò purché sia stata fornita idonea informativa ex art. 13, GDPR e purché i dati siano pertinenti alla finalità di "agevolare l'orientamento, la formazione e l'inserimento professionale" degli alunni e siano trattati esclusivamente per detta finalità e, ad ogni modo, nel rispetto delle "vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati".

«Codice Privacy - Art. 96 (Trattamento di dati relativi a studenti). - 1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonche' le istituzioni di alta formazione artistica e coreutica e le universita' statali o non statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, pertinenti in relazione alle predette finalita' e indicati nelle informazioni rese agli interessati ai sensi dell'articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalita'.

Si consiglia di fare in modo che siano gli stessi alunni a richiedere e autorizzare tale comunicazione, tramite un apposito modulo di richiesta, che eventualmente la scuola può far avere alle famiglie nel corso dell'ultimo anno di studi. In base al principio di minimizzazione, occorre poi evitare di comunicare via e numero, ma solo la località di residenza.

Nota del Garante n. 8515 del 6 marzo 2017 "Indicazioni operative sull'art. 96 del Codice in tema di trattamento dei dati personali degli studenti da parte delle istituzioni scolastiche per finalità di orientamento, formazione e inserimento professionale. Cap. 1 – (…) In questo quadro, possono, ad esempio, essere comunicate o diffuse le seguenti tipologie di informazioni identificative degli studenti: nome, cognome, luogo e data di nascita, così come, l'istituzione scolastica di appartenenza, la classe e la sezione di frequenza, nonché, come richiamato dalla stessa disposizione, gli esiti scolastici, intermedi e finali, che devono essere espressi secondo la specifica disciplina di settore vigente. Devono, invece, considerarsi, in linea generale, eccedenti ulteriori informazioni identificative degli interessati, quali, ad esempio, il codice fiscale o l'indirizzo di residenza. (…)"

DOCUMENTAZIONE PRIVACY DI ISTITUTO

Occorre preparare e mantenere aggiornata e disponibile in caso di controlli la seguente documentazione:

- Informative art. 13 per gli alunni, il personale scolastico e gli esperti esterni
- Nomine e istruzioni ai soggetti autorizzati: personale ATA, docenti, c. scolastici, tutor
- Registro delle attività di trattamento
- Nomine ai Responsabili del trattamento (registro elettronico, segreteria digitale, ecc.)
- Policy Regolamento per l'uso degli strumenti informatici

- Policy e modulistica per l'esercizio dei diritti
- Documento di valutazione dei rischi privacy
- Registro delle violazioni e linee guida data breach
- Atto di designazione del RPD
- Eventuali autorizzazioni all'utilizzo delle immagini
- Clausole contrattuali aggiornate al RGPD

La documentazione, una volta preparata, va messa in opera nel seguente modo:

- Pubblicare le informative art. 13 sul sito internet e preparare una procedura di segreteria per consegnarle ai nuovi alunni, personale scolastico ed esperti esterni
- Consegnare le Nomine e istruzioni ai soggetti autorizzati
- Consegnare la Policy Regolamento per l'uso degli strumenti informatici a chi ha accesso al sistema
- Inviare per PEC le nomine ai Responsabili del trattamento

Tutto il personale scolastico che opera e che tratta dati personali all'interno della scuola assume il ruolo di "Soggetto autorizzato". La designazione deve essere chiara per l'incaricato, il quale deve ricevere inoltre delle istruzioni dal titolare su come comportarsi in merito al trattamento dei dati personali.

GESTIONE DEI DATI PERSONALI NEL SITO INTERNET ISTITUZIONALE

Il sito internet è uno potente strumento per venire a contatto con le famiglie e in generale con l'utenza della scuola, occorre quindi sfruttarne al meglio le potenzialità.

Si consiglia di istituire una sezione "Privacy" raggiungibile facilmente dalla home page, in cui inserire i seguenti elementi:

- I dati di contatto dell'RPD
- le informative privacy in formato PDF
- il modello per l'esercizio dei diritti in materia di protezione dei dati personali
- la cookie policy e la privacy policy del sito

GRADUATORIE

Per il principio di minimizzazione, nei documenti che si pubblicano la scuola deve inserire i soli dati necessari alla finalità perseguita. Nella fattispecie, le graduatorie sono state oggetto di un provvedimento del Garante (Registro dei provvedimenti n. 274 del 6 giugno 2013) https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2535862 il quale ha stabilito che gli unici dati personali che occorre pubblicare sono nome e cognome, posizione e punteggio ed eventuali altri dati strettamente necessari all'individuazione del candidato. Si consiglia quindi di togliere dai file pubblicati eventuali altri dati in eccesso.

MISURE DI SICUREZZA INFORMATICHE EX ART. 32 RGPD

L'utilizzo del sistema informatico deve prevedere un adeguato livello di sicurezza, a protezione dei dati personali in esso contenuti.

Si consiglia quindi di adottare, in accordo i gestori dei vari sistemi utilizzati, le seguenti accortezze:

- un sistema di autenticazione, che deve prevedere l'identificazione dell'utente in modo univoco (user e password). L'accesso ai pc deve avvenire esclusivamente con le proprie credenziali riservate e non con quelle di colleghi. L'accesso alla posta elettronica deve avvenire esclusivamente con l'account assegnato e non con quello di colleghi;
- le password devono avere criteri di complessità ed essere riservate;
- un sistema di autorizzazione ai file office presenti su Server interno in base alle funzioni assegnate ad ogni incaricato;
- utilizzare sistemi informatici aggiornabili per il trattamento delle banche dati;
- predisporre la separazione logica o fisica delle reti didattica e segreteria;
- proteggere il server e le copie di backup da accessi indesiderati;
- proteggere la rete interna da accessi esterni indesiderati;
- applicazione di filtraggi alla navigazione Internet (webfilters);
- applicazione di tecniche di cifratura o pseudonimizzazione;
- accesso controllato alle reti wi-fi tramite autenticazione o password complessa;
- utilizzare antivirus e antispam;
- svolgere regolarmente i salvataggi del server della segreteria;
- aggiungere un secondo sistema di backup, che rimanga sempre spento o scollegato dalla rete in modo che in caso di virus informatico possa costituire un'opzione di recupero dei dati personali;
- verificare la presenza di un gruppo di continuità (UPS) per il server della segreteria;
- dismettere l'hardware della segreteria assicurandosi di aver reso i dati non più accessibili;
- assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano dati personali;
- ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

CONCLUSIONI

Le eventuali situazioni a cui porre attenzione sono segnalate all'interno della sezione "Evidenze privacy", con diversa classificazione a seconda della gravità e dell'urgenza dell'intervento richiesto.

Qualora ne siano presenti, preghiamo il titolare di attivarsi quanto prima per risolvere le evidenze emerse, dandone comunicazione al RPD.

Modena, 02/5/2023

Giampaolo Spaggiari

GIAMPAOLO SPAGGIARI
Data Protection Officer | Consulente Privacy
Certificazione registro TUV Italia n° CDP_231
Conforme ISO/IEC 17024-2012

Nota: questo rapporto è stato elaborato sulla base di quanto evidenziato durante l'attività ispettiva; è possibile che esso non evidenzi possibili altre attività, non conformi alla legge. Nel corso dell'audit, sono state attuate tutte le possibili precauzioni per fare in modo che questo rapporto sia accurato, ma non è possibile accettare responsabilità di sorta, anche nei confronti di parti terze, per qualsiasi perdita o danno che possa nascere, in conseguenza delle situazioni e delle valutazioni, evidenziate in questo rapporto.