



	<p style="text-align: center;">ISTITUTO COMPRENSIVO SCUOLA DELL'INFANZIA SCUOLA PRIMARIA E SECONDARIA DI 1° GRADO "LI PUNTI" VIA ERA - 07100 SASSARI (SS) C. F. 92128460901 - Cod. Mec. SSIC85100T - E-Mail SSIC85100T@istruzione.it TEL.079395658 – FAX. 0793026401 – Codice Univoco UFWICT</p>
---	--

Circ. n° 83 del 25/10/2019

A tutto il personale della scuola
Alla DSGA

Istituto Comprensivo Li Punti

OGGETTO: REGOLAMENTO UE N. 679/2016 – GDPR – PROTEZIONE E TRATTAMENTO DATI. INFORMAZIONE-FORMAZIONE

Si ricorda a tutto il personale in indirizzo che il 25 maggio 2018 è entrato in vigore il Regolamento UE 2016/679, noto come GDPR (General Data Protection Regulation), relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

Anche le scuole sono chiamate ad adeguarsi al **GDPR** e al **D. Lgs. 10 agosto 2018, n. 101**, entrato in vigore lo scorso 19 settembre ed intervenuto ad incidere sul Codice privacy. La necessità è quella di rivedere **l'organizzazione delle attività, non semplicemente in termini formali – attraverso un adeguamento documentale – quanto, piuttosto, a realizzare una rivoluzione culturale** all'interno di molte prassi.

Il Regolamento promuove la responsabilizzazione (*accountability*) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Tutto il personale scolastico (docenti, collaboratori Scolastici, personale di segreteria) è incaricato del trattamento dei dati ai fini istituzionali, ciascuno secondo le proprie competenze.

Si fa presente che tutto il materiale informativo, le linee guida e gli incarichi al riguardo sono pubblicati nel sito della scuola all'indirizzo: <http://www.iclipunti.edu.it/index.php/11-generale/302-sicurezza-e-privacy>

Tutto il personale scolastico è tenuto a prenderne attenta visione per una stretta osservanza e norma.

LE NOVITA' DEL GDPR

Per venire alle novità introdotte dal GDPR c'è prima di tutto da osservare come i principi generali che sono alla base del trattamento dei dati personali (liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza) sono in gran parte gli stessi del DL 196/2003 basato su una direttiva europea (n. 95/46) di oltre vent'anni fa. Nel rispetto complessivo di tali principi, con il Regolamento anche le amministrazioni scolastiche vengono catapultate da un'epoca in cui la maggioranza delle persone si scambiava ancora la corrispondenza con fax e francobolli ad una nuova dimensione pensata per gli scenari più complessi dell'Internet of Things e dei Big Data, in cui anche gli studenti più giovani usano internet ed i social. Ciò ha indotto ad introdurre nel nuovo Regolamento rilevanti novità sul piano della tutela dei diritti delle persone con la previsione di strumenti per responsabilizzare maggiormente le imprese e le amministrazioni. Le nuove regole hanno quindi l'obiettivo di adeguare le norme di protezione dei dati ai cambiamenti determinati dall'incessante evoluzione delle tecnologie e dal conseguente mutamento degli scenari sociali ed economici e di

creare il giusto clima per lo sviluppo del mercato digitale recuperando la fiducia dei cittadini, ai quali sono stati riconosciuti nuovi diritti e maggiore controllo dei loro dati.

LE PRIORITA' DEL GARANTE

Il Garante stesso di fronte alla rilevanza degli impegni e alla mancanza del decreto di armonizzazione della normativa italiana al Regolamento (rinviato, come detto, al 21 agosto 2018) ha individuato le seguenti priorità:

- nomina del Responsabile della Protezione dei Dati (RPD)
- istituzione del Registro dei Trattamenti
- Definizione delle procedure di Data Breach

LA NOMINA DEL RPD

Dal 25 maggio tale figura deve essere presente in tutte le pubbliche amministrazioni e che la mancata nomina, particolarmente grave per il Regolamento, comporta pesanti sanzioni a carico del Dirigente Scolastico.

Come dice il Regolamento UE il RPD è una figura con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali. Il suo ruolo è centrale nell'applicazione della legge perché non solo deve supportare l'amministrazione nel rispetto della normativa ma costituisce punto di contatto per qualunque comunicazione con il Garante o con gli interessati.

Tale figura può essere anche interna all'amministrazione ma deve avere i requisiti sopra richiamati. In ogni caso è escluso che questo ruolo possa essere ricoperto dal Dirigente Scolastico (in quanto titolare del trattamento) o dal DSGA (che potrà invece essere nominato responsabile interno del trattamento).

Di norma le amministrazioni scolastiche devono quindi cercare il proprio RPD fra aziende e liberi professionisti che abbiano l'alta professionalità ed esperienza richiesti dalla normativa e che siano disposti ad assumere tale incarico. La scelta dell'RPD non può essere fatta con leggerezza perché il RPD non funziona da parafulmine per il dirigente riguardo i trattamenti personali operati dall'amministrazione la cui responsabilità rimane sempre a carico del titolare e del responsabile del trattamento che rispondono personalmente in caso di inosservanza del GDPR (Art. 24 delle Linee Guida Gruppo Art. 29) e che devono essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (principio di accountability).

La sfida dell'accountability, anche per la scuola

La vera sfida, anche per il settore dell'istruzione, è rappresentata dal dare concretezza al principio di *accountability* – anche noto come principio di responsabilizzazione – su cui poggia l'intero impianto normativo e, al tempo stesso, evitare la paralisi delle attività delle istituzioni per via di un timore verso le novità introdotte dalla disciplina comunitaria.

Quali sono i principali adempimenti cui sono chiamate le istituzioni scolastiche al fine di adeguarsi all'attuale quadro normativo che va ad incidere innanzitutto sull'organizzazione interna dell'istituto, imponendo una revisione dell'assetto, oramai consolidato, disegnato dal Codice Privacy in epoca antecedente al D.lgs. 101/18?

I soggetti coinvolti nel trattamento dei dati

La revisione che viene richiesta dal GDPR comincia dal novero dei soggetti coinvolti nel trattamento dei dati dal momento che, al di là delle assonanze terminologiche, risultano profondamente incisi i ruoli e le responsabilità attribuiti a ciascuno di essi.

Anche all'interno dell'organigramma dell'Istituto scolastico si dovranno così individuare le figure indicate dal GDPR e dal novellato Codice Privacy e che si possono così elencare:

- titolare del trattamento,
- responsabili (esterni) del trattamento,
- eventuali sub-responsabili, soggetti autorizzati,
- responsabile della protezione dei dati.

Il primo equivoco che va chiarito, per quanto possa suonare scontato agli esperti della materia, è che il titolare del trattamento, ossia il soggetto che determina le finalità e i mezzi del trattamento dei **dati personali**, sarà sempre

l'Istituto scolastico nel suo complesso e non già la persona fisica posta alla sua direzione il cui ruolo sarà quello di dare esecuzione alle determinazioni del titolare.

Si deve subito segnalare che, nel nuovo quadro regolamentare, il titolare del trattamento è chiamato ad assicurare, attraverso scelte non più guidate o suggerite dal legislatore, l'obiettivo del massimo grado di protezione dei dati trattati, dati che, per l'istituzione scolastica, saranno riferiti per lo più ad utenti minorenni. Nell'effettuare queste scelte il titolare dovrà farsi guidare dal principio di *accountability*, o principio di responsabilizzazione, che, nella realtà dei fatti, si tradurrà, ad esempio, nell'accurata selezione dei soggetti cui affidare servizi e forniture avendo riguardo alla sussistenza di garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate e tali da soddisfare i requisiti del GDPR e garantire la tutela dei diritti dell'interessato: nell'individuazione del fornitore – chiamato nello svolgimento del servizio a trattare dati personali – l'Istituto dovrà tener conto, nella valutazione del massimo vantaggio conseguibile, anche del livello di tutela dei dati che il soggetto propone nell'offerta.

È proprio in relazione all'adeguatezza delle misure che si individua uno dei primi cambi di rotta rispetto alla normativa previgente. Il Codice Privacy infatti all'articolo 33 e nell'Allegato B faceva riferimento ad una serie di misure minime – che tutti i titolari erano tenuti ad adottare – volte ad assicurare un livello basilare di protezione dei dati. Il legislatore europeo, invece, ben conscio dell'evoluzione e del progresso tecnologico ha spazzato via il requisito di misure “minime” prevedendo che i titolari adottassero misure adeguate alla protezione dei dati in linea con la realtà in continuo mutamento. Conformemente a tale impostazione e in aderenza a tale inversione di tendenza, l'articolo 27, comma 1, lett. d), del D. Lgs. n. 101/2018 ha abrogato l'Allegato B del Codice Privacy rubricato “Disciplinare tecnico in materia di misure minime di sicurezza”. Ciò non esclude che tale documento possa rappresentare un valido punto di partenza per orientarsi e per poi procedere all'individuazione delle ulteriori misure che, alla luce dello stato della tecnica e delle condizioni specifiche del trattamento, vadano ad integrare il sistema di protezione necessario e conforme a quanto stabilito dal GDPR.

Il legislatore nazionale, all'articolo 2 *quaterdecies* del D.lgs. 196/2003, ha poi previsto che, nell'ambito dell'organigramma organizzativo dell'Istituto, specifici compiti e funzioni connessi al trattamento di dati personali siano demandati ad un ufficio o singolo dipendente – particolarmente qualificato – che, individuato con apposito atto di nomina, potrebbe essere investito dell'esecuzione delle principali operazioni di “privacy policy”. In particolare, tra le tante attività, il designato potrà essere chiamato:

- a coadiuvare la tenuta del registro delle attività di trattamento ai sensi dell'art. 30 par.1 GDPR;
- a coordinare l'attività di aggiornamento delle informative da rendere agli interessati, ai sensi degli artt. 13 e 14 del Regolamento;
- a valutare i soggetti da nominare responsabili del trattamento ai sensi dell'art. 28 GDPR;
- ad assicurare immediato riscontro alle richieste del [DPO](#) riconducibili al settore di appartenenza;
- a coordinare le attività di valutazione degli impatti privacy (Privacy Impact Assessment– PIA) fin dal momento della progettazione dei processi e degli applicativi informatici di supporto, nei casi in cui il trattamento alla base degli stessi, per sua natura, oggetto o finalità, presenti rischi specifici per i diritti e le libertà degli interessati.

In ogni caso, il titolare è chiamato a fornire adeguate istruzioni a tutti quei dipendenti che abbiano accesso a dati personali.

Il Responsabile del trattamento

Tali figure, in linea con quanto previsto dall'art. 29 del GDPR, potrebbero essere indicati come delegati o incaricati al trattamento ma non vanno confusi con il “responsabile interno”, figura tutta italiana e sconosciuta alla normativa comunitaria e che, allo stato, dobbiamo ritenere scomparsa. Il Regolamento UE 2016/679, invero, all'articolo 28 GDPR si occupa del “Responsabile del Trattamento”, inteso come soggetto che tratta i dati per conto del Titolare, le cui significative peculiarità si colgono nell'articolata disciplina che il GDPR gli riserva. Dalla lettura complessiva dell'articolo emerge la figura di un soggetto – persona fisica, giuridica, autorità pubblica, servizio od organismo – che si pone all'esterno dell'organizzazione del titolare e per conto del quale, con una discrezionalità più o meno ampia, tratta i dati e persegue le finalità definite dallo stesso. Il responsabile al trattamento – la cui nomina, nei termini essenziali richiesti dall'art. 28 GDPR, dovrà avere forma scritta sia quale atto autonomo o, in alternativa, con l'inserimento di una clausola ad hoc all'interno del contratto di servizio – dovrà presentare garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento affidato soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.

Il sub-responsabile del trattamento

Nelle operazioni di trattamento affidate dal titolare al responsabile quest'ultimo si potrà servire, a sua volta, di un altro soggetto per il compimento di specifiche attività nell'ambito del trattamento che compie per conto del titolare. In questo caso, il responsabile – previa autorizzazione scritta del titolare⁴¹ – procederà a nominare tale soggetto quale sub-responsabile del trattamento obbligandolo ad osservare gli stessi obblighi, in materia di protezione dei dati, che gravano su di lui nel rapporto con il titolare.

Qualora il responsabile non provveda ad impartire al sub-responsabile le istruzioni previste, così come nel caso in cui il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Il responsabile della protezione dei dati

Una figura completamente nuova è invece quella del responsabile della protezione dei dati (RPD o, secondo l'acronimo inglese *DPO – Data Protection Officer*), la cui nomina è obbligatoria per tutte le autorità e gli organismi pubblici dunque anche per gli istituti scolastici

Compiti dell'RPD:

- informare e fornire consulenza al titolare;
- curare la formazione del personale;
- sorvegliare l'osservanza della normativa;
- fornire un parere in merito alle valutazioni d'impatto (se richiesto);
- cooperare con l'autorità di controllo (che in Italia è il Garante per la protezione dei dati personali);
- fungere da punto di contatto tra l'autorità e il titolare.

Il titolare è tenuto a fornire al RPD tutte le risorse di cui necessita per l'esecuzione dei suoi compiti e non può penalizzarlo o rimuoverlo a seguito dell'adempimento degli stessi. Ciò non toglie che, all'esito di pareri espressi dal RPD, che ricordiamo non essere vincolanti, il titolare possa operare in senso opposto, fermo restando il principio di responsabilizzazione. L'onere di assicurare il rispetto della normativa e la conformità delle operazioni di trattamento al GDPR ricade sempre sul titolare poiché il responsabile della protezione dei dati non risponde personalmente in caso di inosservanza del GDPR.

Come abbiamo innanzi detto, il RPD può essere sia interno che esterno all'Istituto e, nel primo caso, potendo svolgere altre funzioni all'interno dell'Istituto, dovrà farsi particolare attenzione alla sussistenza, anche solo potenziale, di un conflitto d'interessi (art. 38 par. 6 GDPR). Nel caso di RPD esterno, invece, l'Ente dovrà stipulare un vero e proprio contratto di servizi all'esito di una procedura selettiva in cui si indicheranno i requisiti di partecipazione, la durata e le caratteristiche di esecuzione della prestazione.

La designazione del RPD ed i suoi dati di contatto dovranno essere comunicati dal titolare al Garante mediante [la procedura telematica](#) messa a disposizione sul sito al seguente indirizzo.

I principali adempimenti

Al pari delle figure sin qui illustrate, gli adempimenti e le attività che l'Istituzione scolastica è chiamata a compiere per adeguarsi al nuovo quadro normativo, non paiono presentare particolari peculiarità rispetto a quanto dovranno realizzare le altre pubbliche amministrazioni. Di seguito proveremo ad illustrarle segnalando le eventuali specificità del caso.

Oltre alla designazione dell'RPD, le scuole devono:

Aggiornare le informative

Una delle prime operazioni da compiersi è sicuramente l'aggiornamento delle informative da rendere agli interessati nel rispetto degli articoli 13 e 14 GDPR, con l'indicazione dei nuovi requisiti richiesti. La forma con cui deve essere resa l'informativa è individuata dal GDPR nella forma scritta o anche con mezzi elettronici: è evidente che il requisito potrà ritenersi integrato con la pubblicazione dell'informativa sul sito web

dell'Istituto. Sarà bene redigere informative non eccessivamente strutturate che potrebbero veder compromesso il requisito della chiarezza e della semplicità optando, se del caso, per una pluralità di informative ritagliate sulla categoria di interessati cui saranno dirette (alunni/famiglie da un lato, dipendenti dall'altro, fornitori etc.). Il contenuto dell'informativa è indicato dal GDPR che, tra le novità, richiede l'indicazione del periodo di conservazione dei dati, la base giuridica su cui si fonda il trattamento ai sensi dell'art. 6 GDPR, l'ampio ventaglio dei diritti riconosciuti all'interessato e l'indicazione dei dati di contatto del responsabile della protezione dei dati. La categoria degli interessati, ricordiamolo, nell'ambito degli istituti scolastici è costituita perlopiù da soggetti minorenni che, dunque, non possono rilasciare alcun valido consenso al trattamento dei dati fino al compimento del 18 anno di età. Qualora lo studente dovesse raggiungere la maggiore età nel corso del ciclo scolastico sarà necessario acquisire il consenso direttamente dall'interessato e non dai genitori o dai soggetti che ne hanno precedentemente esercitato la potestà genitoriale.

In tema di consenso del minore, dobbiamo inoltre ricordare che il GDPR, al considerando 38, stabilisce chiaramente che *“il consenso del titolare della responsabilità genitoriale non deve essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente ai minori”* con lo scopo di evitare qualunque ostacolo alla fruizione da parte del minore di servizi pensati e predisposti per la sua tutela quali, ad esempio, lo sportello di ascolto presente in diverse scuole per la lotta contro cyber bullismo, o, più in generale, di sostegno all'infanzia e ai minori nel contesto relazionale scolastico e familiare.

Le informative andranno dunque così rese dall'Istituto e non sarà necessario acquisire il consenso degli interessati salvo non siano effettuati trattamenti di dati che necessitino di essere espressamente autorizzati. Tali sono, per cominciare, le “famigerate” foto nel corso degli eventi dell'Istituto: l'interessato dovrà esprimere il proprio consenso non solo a che l'istituto effettui le riprese audio foto e video (raccolta) ma anche a che l'Istituto le comunichi o diffonda (pubblicazione on line sul sito d'istituto).

Passando all'esame di alcune specificità che l'ambito scolastico presenta, si segnala che il periodo di conservazione dei dati deve essere individuato sulla scorta del principio in base al quale i dati personali possono essere conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti. Tuttavia, nell'ambito della PA, per l'individuazione dei tempi di conservazione dei dati da indicare nell'informativa questi sono comunque stabiliti per legge e si dovrà tenere in debito conto di quanto disposto in materia di archivi delle istituzioni scolastiche dal Ministero dei Beni e delle Attività culturali.

La nomina e i rapporti con i responsabili del trattamento

L'istituzione scolastica, fa spesso ricorso a soggetti che forniscono prestazioni di supporto o strumentali all'esercizio dei compiti propri dell'Istituto stesso. In tal caso, qualora la prestazione comporti il trattamento di dati personali da parte del fornitore, anche non come oggetto specifico della prestazione, questo dovrà essere nominato responsabile del trattamento ai sensi dell'art. 28 del GDPR in tutti i casi in cui tratti dati personali per conto del titolare. Ciò comporta la necessità di disciplinare il rapporto con il fornitore anche sotto questo specifico aspetto a mezzo di clausole del contratto o con altro atto giuridico *a latere allo stesso* a norma dell'Unione o degli Stati membri che vincoli il responsabile al titolare. In tale atto, si dovrà regolamentare la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e delle responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato. Nella nomina, il titolare, nell'ottica di rispettare il principio di *accountability*, detterà delle istruzioni al responsabile. A titolo esemplificativo, prevederà che il responsabile:

- tratti i dati personali soltanto su sua istruzione documentata;
- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti le misure richieste ai sensi dell'articolo 32 GDPR;
- assista il titolare nel dare riscontro alle richieste di esercizio dei diritti avanzate dagli interessati e lo informi tempestivamente nel caso in cui si verifichi una violazione di dati personali.

La tenuta del registro delle attività di trattamento

Un altro adempimento che l'Istituto, in qualità di titolare del trattamento, è chiamato ad assolvere è quello relativo alla tenuta del registro delle attività di trattamento secondo quanto previsto dall'art. 30 par. 1 GDPR.

Si tratta di un documento di censimento e analisi contenente le principali informazioni relative alle operazioni di trattamento effettuate che si configura come una “fotografia” sullo stato attuale dei trattamenti posti in essere.

Esso deve avere forma scritta, anche elettronica e, quando richiesto, deve essere esibito su richiesta del Garante. Ovviamente, dal momento che il registro deve essere sempre mantenuto aggiornato, qualsiasi cambiamento deve essere inserito provvedendo, così come suggerito dal Garante nelle FAQ dell'8 ottobre 2018 ad annotare sia la data di creazione che la data dell'ultimo aggiornamento. Si suggerisce, inoltre, di assegnare una data certa al documento, per mezzo di strumenti adeguati (a titolo esemplificativo: marche temporali, ma potrebbero essere sufficiente anche messaggi di posta elettronica certificata).

A norma dell'art. 30 par. 1 GDPR, il registro deve contenere:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Oltre a quanto espressamente previsto dal par. 1, all'interno del documento è possibile inserire qualsiasi altra informazione ritenuta utile da parte del titolare nel rispetto del citato principio di *accountability* (ad es. le modalità di raccolta del consenso, le eventuali valutazioni di impatto effettuate, l'indicazione di eventuali "referenti interni" individuati dal titolare in merito ad alcune tipologie di trattamento ecc.).

Per le istituzioni scolastiche il Miur, con nota n. 877 del 03/08/2018, ha trasmesso alle scuole uno schema di Registro delle attività di trattamento corredato da una guida operativa per la compilazione dei campi individuati. La metodologia utilizzata per la compilazione del Registro delle attività di trattamento ha consentito di individuare i principali processi gestiti dalle istituzioni scolastiche.

Pare opportuno precisare che il modello andrà integrato con quei trattamenti ulteriori – sia per finalità che per tipologia di dati – che il singolo istituto effettua nello specifico quali acquisizione di foto, creazione e gestione di account per gli studenti e dipendenti, newsletter et c..

Altrettanto utili sono le linee guida sul [Registro delle attività di trattamento](#) messe a disposizione dal Garante Privacy.

La conduzione delle valutazioni d'impatto

Sebbene abbiamo più volte ricordato che la scuola effettui trattamenti consentiti e guidati dalle disposizione di legge o di regolamento, ciò non esclude che possa essere necessario effettuare una valutazione degli impatti privacy (Privacy Impact Assessment– PIA) e, specificatamente, che ciò avvenga nei casi in cui, fin dal momento della progettazione dei processi e degli applicativi informatici di supporto, il trattamento alla base degli stessi, per sua natura, oggetto o finalità, presenti rischi specifici per i diritti e le libertà degli interessati.

Tra le ipotesi che ad oggi si possono prendere in considerazione ricordiamo, ad esempio, l'adozione di sistemi di rilevazione biometrica delle presenze (rilievo delle impronte).

LA DIRIGENTE SCOLASTICA

Dott.ssa M. P. Teresa Useri

Firma autografa sostituita a mezzo stampa

Ai sensi dell'art. 3, comma 2, D.lvo 39/93