Istituto Comprensivo Statale
Anastasio De Filis - Terni

Registro delle Attività di Trattamento
Regolamento EU 679/2016 GDPR

ENTE TITOLARE DEL TRATTAMENTO	
Denominazione	ICS Anastasio De Filis
Indirizzo	Via Anastasio de Filis
CAP e Città (Prov)	05100 – Terni - TR
Telefono	0744-425590
Email	Tric811001@istruzione.it
PEC	Tric811001@pec.istruzione.it
Titolare	Dirigente Scolastico pro tempore
Data Controller	Direttore S.G.A. pro tempore

RESPONSABILE PROTEZIONE DEI DATI (RPD/DPO)	
Denominazione	**Easyteam.org SRL**
Nominativo	Bassi Ferdinando
Indirizzo	Piazza Lorenzo Perosi, 6
CAP e Città (Prov)	26866 Sant'Angelo Lodigiano (LO)
Email	**rpd@easyteam.org**
PEC	**easyteam@easypec.org**
Telefono	0371.21.04.04

ELENCO REVISIONI		
01/06/2018	1.0	Revisione iniziale
22/08/2018	1.1	Rivista impaginazione grafica
29/09/2018	1.2	Aggiunte definizioni; migliorata descrizione dei trattamenti in atto
09/04/2020	2.0	Aggiunte le valutazioni di impatto per i trattamenti relativi alla Didattica a Distanza (DaD)
14/05/2020	3.0	Aggiunti i criteri di valutazione dei rischi (DPIA)
14/05/2020	3.1	Aggiunte le valutazioni dei rischi per i trattamenti censiti (DPIA)
20/08/2022	3.2	Aggiunta la valutazione dei rischi per la piattaforma Google Workspace a seguito della modifica dei termini contrattuali

Sommario

Introduzione

Il presente Registro dei Trattamenti (di seguito “Registro”) è adottato ai sensi dell’Art. 30 del Regolamento Europeo 2016/679 (di seguito “Regolamento”), per tracciare le attività di trattamento in materia di dati personali, i criteri organizzativi adottati e le misure per la protezione dei dati personali. In particolare il Registro dei Trattamenti contiene idonee informazioni riguardo:

- 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, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- 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 di cui all'articolo 32, paragrafo 1.

Il Registro è tenuto in forma scritta, anche in formato elettronico.

Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Gli obblighi di tenuta del Registro non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 del Regolamento.

T01 - Finalità del trattamento: Gestione del Personale Docente – Contrattualizzazione

Descrizione

Il processo "Gestione del personale docente – contrattualizzazione" comprende tutte le attività di trattamento di dati che sono effettuate dall'istituzione scolastica ai fini dell'assunzione del personale docente.
In particolare, il Dirigente scolastico provvede alla stipula dei contratti per l'assunzione del personale di ruolo e non di ruolo.
Per quanto concerne le assunzioni a tempo indeterminato e le assunzioni a tempo determinato (supplenze annuali entro il 31 agosto), il contratto è stipulato tra il docente e il dirigente scolastico, in qualità di delegato del dirigente dell'Ufficio Scolastico Regionale.
Per le assunzioni per supplenze brevi e saltuarie, il contratto è stipulato tra il docente e il dirigente scolastico, in qualità di legale rappresentante dell'istituzione scolastica.
Alla luce di quanto sopra esposto, è utile sottolineare come il dirigente scolastico si trovi ad operare nella doppia veste di organo dell'amministrazione dello Stato (nel caso di stipula di contratto a tempo indeterminato o di tempo determinato) e di organo dell'istituzione scolastica (nel caso di stipula di contratto per supplenze brevi e saltuarie), allorché eserciti le sue competenze nell'ambito delle funzioni statali ovvero di quelle autonomamente attribuite alle istituzioni scolastiche.

Rispetto al processo analizzato, sono state individuate tre attività:

- Gestione contratto a tempo indeterminato - Personale docente
- Gestione contratto a tempo determinato - Personale docente
- Gestione contratto per supplenze brevi e saltuarie - Personale docente

1. L'attività "Gestione contratto a tempo indeterminato - Personale docente" prevede il trattamento di tutti dati personali funzionali al perfezionamento dell'assunzione del personale docente a tempo indeterminato, con riferimento agli aspetti relativi al trattamento giuridico ed economico, nonché alla verifica del possesso dei requisiti per l'assunzione.
Tale attività comporta una contitolarità ex art. 26 del Reg. (UE) 2016/679 del MIUR e dell'istituzione scolastica nel trattamento dei relativi dati personali.
Inoltre, i dati personali trattati nell'ambito di questa attività sono gestiti attraverso il portale SIDI e, pertanto, ne consegue che il responsabile esterno del trattamento, ovvero la persona giuridica, che tratta dati personali per conto del titolare, è il fornitore del sistema informativo del MIUR.

2. L'attività "Gestione contratto a tempo determinato - Personale docente" prevede il trattamento di tutti i dati personali funzionali all'assunzione del personale docente a tempo determinato, con riferimento agli aspetti relativi al trattamento giuridico ed economico, nonché alla verifica del possesso dei requisiti per l'assunzione.
Tale attività comporta una contitolarità ex art. 26 del Reg. (UE) 2016/679 del MIUR e dell'istituzione scolastica nel trattamento dei relativi dati personali.
Inoltre, i dati personali trattati nell'ambito di questa attività sono gestiti attraverso il portale SIDI e, pertanto, ne consegue che il Responsabile esterno del trattamento ovvero la persona giuridica, che tratta dati personali per conto del titolare, è il fornitore del sistema informativo del MIUR.

3. L'attività "Gestione contratto per supplenze brevi e saltuarie - Personale docente" prevede il trattamento di tutti i dati personali funzionali all'assunzione del personale docente per supplenze brevi e saltuarie, con riferimento agli aspetti relativi al trattamento giuridico ed economico, nonché alla verifica del possesso dei requisiti per l'assunzione.
Tale attività comporta la titolarità esclusiva dell'istituzione scolastica nel trattamento dei relativi dati personali e il MIUR si pone come responsabile esterno del trattamento, in quanto autorità pubblica che, attraverso l'applicativo del portale SIDI messo a disposizione, tratta dati personali per conto del titolare del trattamento.

Categorie di interessati e categorie di dati personali

- personale docente a tempo determinato ed indeterminato;
- dati anagrafici degli insegnanti a tempo indeterminato, insegnanti a tempo determinato, insegnanti esterni incaricati di funzioni nella scuola: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.;
- dati dei familiari degli insegnanti a tempo indeterminato, insegnanti a tempo determinato, insegnanti esterni incaricati di funzioni nella scuola;
- dati relativi alle assenze per malattia;
- dati relativi alle assenze per permessi familiari (congedi parentali) e per ragioni di studio/formazione/aggiornamento;
- dati relativi ai permessi per familiari portatori di handicap riconosciuto (Legge 104/92, L. 53/2000);
- dati relativi ai permessi per maternità/paternità;
- dati relativi ai permessi sindacali/amministrativi;
- dati relativi alle ferie;
- dati relativi all'analisi delle situazioni di carriera (certificato di servizio e dichiarazione dei servizi prestati);
- contratti di lavoro;
- dati inerenti alla retribuzione/stipendi (dati bancari);
- titoli di studio, dati sul grado di istruzione;
- dati relativi alle altre attività eventualmente svolte dal personale docente;
- comunicazioni al personale necessarie alla gestione amministrativa del rapporto lavorativo (lettere, circolari, avvisi, ecc.);
- dati relativi alla gestione del contenzioso e dei procedimenti disciplinari;
- convocazioni in tribunale;
- dati relativi ai permessi per la donazione del sangue;
- dati relativi ai permessi non retribuiti per i supplenti;
- dati relativi ai permessi previsti dagli artt. 15, 16 DEL CCNL 29/11/07;
- dati necessari per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero della Pubblica Istruzione e dell'ordinamento scolastico;
- dati relativi alla partecipazione a scioperi;
- dati relativi alla partecipazione ad assemblee sindacali.

Natura dei dati

I dati trattati sono di natura comune, sensibile (dati idonei a rivelare le convinzioni religiose, filosofiche, sindacali, d'altro genere; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso; dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro; gestione del contenzioso e procedimenti disciplinari; dati idonei a rivelare la vita sessuale, esclusivamente in caso di rettificazione di attribuzione di sesso) e dati di carattere giudiziario (gestione del contenzioso e procedimenti disciplinari). Il trattamento concerne tutti i dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro.
I dati inerenti lo stato di salute sono trattati per: l'adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzioni del personale appartenente alle c.d. categorie protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative pensionistiche, e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni e/o sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi per il personale e provvidenze, collegati a particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale;
I dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;
I dati sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione.
I dati sulle convinzioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;
I dati di carattere giudiziario sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato.
Le informazioni sulla vita sessuale possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso.

Ambito di comunicazione dei dati

- MIUR, Ufficio Scolastico Regionale, Ufficio Scolastico Provinciale;
- altri Istituti Scolastici, Enti di formazione;
- Ufficio di collocamento (dati dei supplenti, dati anagrafici, dati sul grado d'istruzione, durata della supplenza);
- Direzione Provinciale dei Servizi Vari (tesoreria), Ragioneria Provinciale dello Stato;
- INPS, INDIRE, Ministero dell'Economia;
- sindacati che con domanda motivata richiedano dati relativi ad attività esclusivamente connessa alle loro funzioni;
- assicurazioni private, INAIL, Revisore contabile, A.S.S.;
- musei, teatri, agenzie di viaggi, fondazioni;
- Comune, Provincia, Regione ed altri Enti Pubblici, anche per il personale assunto obbligatoriamente ai sensi della L. 68/1999;

- Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;
- Organi preposti al riconoscimento della causa di servizio/equo indennizzo» ai sensi del DPR 461/2001;
- Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (d.lg. n. 81/2008)
- Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del DPR. n. 1124/1965;
- Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
- Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
- Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003 , n. 186;
- Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e DPR 20 febbraio 1998, n.38;
- Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413;
- MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335.
- Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, d.lg. n. 165/2001);
- Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D.Lgs. 30 marzo 2001, n. 165;
- Organi arbitrali: per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore;
- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di Giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS
- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è:

- esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
- esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso

Trattamento dei dati

Data Controller: Direttore S.G.A.
Data Processor: Assistenti amministrativi

Valutazione dei rischi

Il trattamento ha luogo all'interno degli uffici amministrativi. I dati vengono archiviati in sistemi adeguatamente protetti, vengono gestiti da strumenti software di produttori certificati AgID Marketplace per le PA e vengono trasmessi ad altri portali istituzionali attraverso canali sicuri di comunicazione e scambio dati.

	Descrizione del rischio	**Valutazione di rischio e contromisure da adottare**
Rischio 1	Perdita dei dati a seguito di hardware failure	Basso se l'Istituto è dotato di un sistema di disaster recovery Alto se l'Istituto non è dotato di un sistema di disaster recovery
Rischio 2	Furto di dati	Basso
Rischio 3	Intercettazione dei dati durante la trasmissione	Basso
Rischio 4	Accesso non autorizzato ai dati	Basso se l'istituto ha attivato la gestione di credenziali di accesso personali e ha correttamente sensibilizzato il personale

Soggetti coinvolti	**Modalità**
Direttore S.G.A.	Sensibilizzazione del personale amministrativo
Amministratore di Sistema	Verifica sussistenza delle misure adeguate di sicurezza tecnica e sistemistica

T02 - Finalità del trattamento: Gestione delle Iscrizioni

Descrizione

Il processo "Gestione Iscrizioni" consente ai genitori o a chi esercita la responsabilità genitoriale, dopo essersi registrato sul sito del Ministero dell'istruzione, dell'università e della ricerca (di seguito MIUR) e aver ottenuto le credenziali di accesso, di compilare l'apposito modulo on line al fine di iscrivere lo studente alle classi iniziali dei percorsi scolastici presso le scuole di ogni ordine e grado (scuola primaria, secondaria di primo grado e secondaria di secondo grado). Sono escluse da tale procedura le iscrizioni alla scuola dell'infanzia per le quali è prevista la modalità cartacea.
In tale fase, attraverso l'applicativo SIDI, le istituzioni scolastiche possono prendere visione delle domande di iscrizione pervenute e, eventualmente, fornire supporto alle famiglie nell'inserimento delle domande.
In seguito alla chiusura delle iscrizioni on line, le istituzioni scolastiche provvedono alla gestione e alla verifica delle domande pervenute. Nello specifico, attraverso apposite funzioni rese disponibili sul SIDI, le scuole devono accettare o smistare le domande di iscrizione pervenute. Nel caso in cui le domande pervenute eccedano il limite massimo dei posti complessivamente disponibili, viene predisposta la graduatoria sulla base dei criteri di priorità stabiliti da ogni Istituto. Le domande non accolte sono indirizzate, tramite l'applicativo SIDI, verso gli istituti di seconda o terza scelta.
Al fine di perfezionare l'iscrizione, l'istituzione scolastica può richiedere ai genitori dell'alunno o a chi esercita la responsabilità genitoriale di fornire la documentazione aggiuntiva (obbligatoria o facoltativa), necessaria per la successiva gestione amministrativa dell'alunno con riferimento ai servizi connessi alla didattica.
Rispetto al processo analizzato, in funzione della categoria di dati trattati (ad es. le categorie particolari di dati personali), delle finalità di trattamento (es. predisposizione delle graduatorie, smistamento e accettazione delle domande di iscrizione vs perfezionamento dell'iscrizione), della tipologia, nonché della modalità di trattamento (es. applicativo SIDI vs pacchetto locale), sono state individuate due attività:

1. Iscrizioni – Acquisizione e gestione domande
2. Iscrizioni – Acquisizione documentazione aggiuntiva

1. L'attività "Iscrizioni – Acquisizione e gestione domande" prevede la raccolta delle iscrizioni presentate on line o in modalità cartacea, ove previsto, effettuate dai genitori o da chi esercita la responsabilità genitoriale e la gestione delle stesse al fine di predisporre le graduatorie, accettare o smistare le domande di iscrizione pervenute sulla base della disponibilità di posti e dei criteri di precedenza, deliberati dai singoli Consigli di Istituto.
Le informazioni raccolte per le finalità sopra citate contengono dati comuni e categorie particolari di dati personali (es. lo stato di salute). Tali dati sono trattati mediante l'utilizzo di applicativi informatici, attraverso apposite funzioni rese disponibili sul portale SIDI e, ove presenti, attraverso l'utilizzo di pacchetti locali, nonché, nei casi previsti, in modalità cartacea.
In particolare, nel caso in cui l'istituzione scolastica utilizzi le funzioni del portale SIDI, il MIUR si pone come Responsabile esterno del trattamento, in quanto autorità pubblica che, attraverso l'applicativo messo a disposizione, tratta dati personali per conto del titolare del trattamento che è in via esclusiva l'istituzione scolastica.
Nel caso in cui l'istituzione scolastica utilizzi pacchetti locali, il responsabile del trattamento è il fornitore informatico scelto dall'istituzione scolastica.

Nelle ipotesi di esclusione di gestione delle iscrizioni dal sistema di iscrizioni on line previste dalla relativa Circolare annuale MIUR, le istituzioni scolastiche che trattano dati personali in modalità cartacea sono in via esclusiva titolari del trattamento e non è presente un responsabile del trattamento.

2. L'attività "Iscrizioni – Acquisizione documentazione aggiuntiva" prevede la raccolta della documentazione (obbligatoria o facoltativa) per il perfezionamento dell'iscrizione e per la successiva gestione amministrativa dell'alunno con riferimento anche ai servizi connessi alla didattica.
Le informazioni raccolte per le finalità sopra citate contengono dati comuni e categorie particolari di dati personali (es. lo stato di salute, le convinzioni religiose, filosofiche o di altro genere). Tali dati sono trattati in modalità cartacea e/o mediante l'utilizzo di pacchetti locali.
Il Responsabile esterno del trattamento, ovvero la persona giuridica che tratta dati personali per conto del titolare del trattamento, è il fornitore dei sistemi informativi della scuola.

Categorie di interessati e categorie di dati personali

- alunni ed ex-alunni
- dati anagrafici degli alunni: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.;
- dati personali dei familiari degli alunni;
- dati relativi alle assenze;
- certificati medici;
- valutazione dell'alunno;
- diplomi ed attestati;
- scelta relativa all'ora di religione;
- curriculum scolastico (promozioni, bocciature);
- comunicazioni tra scuola e studente/famiglia dello studente;
- tasse scolastiche (esoneri); dati relativi alla gestione del contenzioso;
- dati relativi ad eventuali handicap;
- dati comunicati da Tribunali dei minorenni, Tribunali, Assistenti sociali;
- lettere e comunicazioni alle famiglie;
- fotografie, riprese audio-video (eventuali).

I dati sopra descritti riguardano anche gli ex allievi dell'Istituto: tali dati sono conservati per il periodo previsto dalla legge.

Natura dei dati

I dati trattati sono di natura comune, sensibile (dati idonei a rivelare l'origine razziale o etnica, per favorire l'integrazione degli alunni stranieri; dati idonei a rivelare le convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento; dati idonei a rivelare le convinzioni filosofiche, politiche, d'altro genere, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei familiari; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso, per assicurare l'erogazione del sostegno agli alunni disabili, dell'insegnamento

domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate a quelle motorie e sportive, alle visite guidate e ai viaggi d'istruzione, all'erogazione del servizio mensa) e dati a carattere giudiziario (nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno e/o della famiglia dell'alunno, oppure per la gestione del contenzioso con le famiglie degli alunni).

Ambito di comunicazione dei dati

- MIUR, Ufficio Scolastico Provinciale, Ufficio Scolastico Regionale, INVALSI;
- assicurazioni private, INAIL, ASS;
- Consolati, direttori centri cultura esteri;
- musei, teatri, agenzie di viaggi, fondazioni;
- Procura della Repubblica, Tribunale dei minori, Tribunale;
- Comune, Provincia, Regione ed altri Enti Pubblici per la fornitura dei servizi ai sensi del D. Lgs. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
- S.I.D.D.I.F. - Sistema informativo per il Diritto/Dovere all'Istruzione e alla Formazione (contenente l'Anagrafe degli studenti e l'Osservatorio sulla scolarità);
- gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
- altri Istituti Scolastici, statali e non, enti di formazione;
- ad aziende, imprese e altri soggetti pubblici e/o privati per tirocini formativi, stages e alternanza scuola-lavoro ai sensi della Legge 24 giugno 1997, n. 196 e del D. Lgs. 21 aprile 2005 n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizi;
- Associazioni Sportive, Professionisti (per specifici progetti);
- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di Giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS
- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.

I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è l'esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale

Trattamento dei dati

Data Controller: Direttore S.G.A.
Data Processor: Assistenti amministrativi

Valutazione dei rischi

Il trattamento ha luogo all'interno degli uffici amministrativi. I dati vengono archiviati in sistemi adeguatamente protetti, vengono gestiti da strumenti software di produttori certificati AgID Marketplace per le PA e vengono trasmessi ad altri portali istituzionali attraverso canali sicuri di comunicazione e scambio dati.

	Descrizione del rischio	**Valutazione di rischio e contromisure da adottare**
Rischio 1	Perdita dei dati a seguito di hardware failure	Basso se l'Istituto è dotato di un sistema di disaster recovery Alto se l'Istituto non è dotato di un sistema di disaster recovery
Rischio 2	Furto di dati	Basso
Rischio 3	Intercettazione dei dati durante la trasmissione	Basso
Rischio 4	Accesso non autorizzato ai dati	Basso se l'istituto ha attivato la gestione di credenziali di accesso personali e ha correttamente sensibilizzato il personale

Soggetti coinvolti	**Modalità**
Direttore S.G.A.	Sensibilizzazione del personale amministrativo
Amministratore di Sistema	Verifica sussistenza delle misure adeguate di sicurezza tecnica e sistemistica

T03 - Finalità del trattamento: Gestione degli Alunni

Descrizione

Il processo "Gestione della carriera scolastica degli alunni" comprende tutte le attività di trattamento di dati personali che sono effettuate dall'istituzione scolastica per la gestione del percorso scolastico, formativo e amministrativo dell'alunno.
A tal fine, le istituzioni scolastiche acquisiscono, gestiscono e conservano, sotto la propria responsabilità, la documentazione, necessaria per lo svolgimento di tutte le attività relative alla carriera scolastica e al rapporto con gli alunni, nella quale sono presenti anche dati personali.
Tutta la documentazione acquisita nell'ambito della gestione della carriera scolastica dell'alunno confluisce nel fascicolo dello studente, il quale può essere tenuto sia in modalità cartacea che in modalità elettronica (nel caso in cui l'istituzione scolastica si avvalga dell'applicativo SIDI o disponga di un pacchetto locale).

Rispetto al processo analizzato è stata individuata un'unica attività di trattamento:

1. Gestione dati alunni

Tale attività prevede:
- il trattamento di dati personali relativi al percorso scolastico, formativo e amministrativo dell'alunno per la gestione dello studente, anche in relazione all'erogazione di servizi aggiuntivi;
- l'alimentazione e l'aggiornamento dell'Anagrafe Nazionale degli Studenti al fine di adempiere agli obblighi previsti dal D.M. 692/2017.

Tali dati sono trattati mediante l'utilizzo di applicativi informatici e, nello specifico, attraverso apposite funzioni rese disponibili sul portale SIDI e/o, ove presenti, attraverso l'utilizzo di pacchetti locali.
In particolare, nel caso in cui l'istituzione scolastica utilizzi le funzioni del portale SIDI, il MIUR si pone come responsabile esterno del trattamento, in quanto autorità pubblica che, attraverso l'applicativo messo a disposizione, tratta dati personali per conto del titolare del trattamento che è in via esclusiva l'istituzione scolastica.
Nel caso in cui l'istituzione scolastica utilizzi pacchetti locali, il responsabile del trattamento è il fornitore scelto dalla stessa istituzione scolastica.
Nei casi in cui la "Gestione della carriera scolastica degli alunni" avvenga in via esclusiva in modalità cartacea, le istituzioni scolastiche sono titolari del trattamento e non è presente il responsabile del trattamento.

Categorie di interessati e categorie di dati personali

- alunni ed ex-alunni, minorenni e maggiorenni
- dati anagrafici degli alunni: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.;
- dati personali dei familiari degli alunni;
- dati relativi alle assenze;
- certificati medici;
- valutazione dell'alunno;

- diplomi ed attestati;
- scelta relativa all'ora di religione;
- curriculum scolastico (promozioni, bocciature);
- comunicazioni tra scuola e studente/famiglia dello studente;
- tasse scolastiche (esoneri); dati relativi alla gestione del contenzioso;
- dati relativi ad eventuali handicap;
- dati comunicati da Tribunali dei minorenni, Tribunali, Assistenti sociali;
- lettere e comunicazioni alle famiglie;
- fotografie, riprese audio-video (eventuali).

I dati sopra descritti riguardano anche gli ex allievi dell'Istituto: tali dati sono conservati per il periodo previsto dalla legge.

Natura dei dati

I dati trattati sono di natura comune, sensibile (dati idonei a rivelare l'origine razziale o etnica, per favorire l'integrazione degli alunni stranieri; dati idonei a rivelare le convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento; dati idonei a rivelare le convinzioni filosofiche, politiche, d'altro genere, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei familiari; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso, per assicurare l'erogazione del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate a quelle motorie e sportive, alle visite guidate e ai viaggi d'istruzione, all'erogazione del servizio mensa) e dati a carattere giudiziario (nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno e/o della famiglia dell'alunno, oppure per la gestione del contenzioso con le famiglie degli alunni).

Ambito di comunicazione dei dati

- MIUR, Ufficio Scolastico Provinciale, Ufficio Scolastico Regionale;
- INVALSI;
- assicurazioni private, INAIL, ASS;
- Consolati, direttori centri cultura esteri;
- musei, teatri, agenzie di viaggi, fondazioni;
- Procura della Repubblica, Tribunale dei minori, Tribunale;
- Comune, Provincia, Regione ed altri Enti Pubblici per la fornitura dei servizi ai sensi del D. Lgs. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
- S.I.D.D.I.F. - Sistema informativo per il Diritto/Dovere all'Istruzione e alla Formazione (contenente l'Anagrafe degli studenti e l'Osservatorio sulla scolarità);
- gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;

- altri Istituti Scolastici, statali e non, enti di formazione;
- ad aziende, imprese e altri soggetti pubblici e/o privati per tirocini formativi, stages e alternanza scuola-lavoro ai sensi della Legge 24 giugno 1997, n. 196 e del D. Lgs. 21 aprile 2005 n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizi;
- Associazioni Sportive, Professionisti (per specifici progetti);
- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di Giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS
- invio periodico del modello MMS al Responsabile della protezione dei dati

- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è l'esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale

Trattamento dei dati

Data Controller: Direttore S.G.A.
Data Processor: Assistenti amministrativi

Valutazione dei rischi

Il trattamento ha luogo all'interno degli uffici amministrativi. I dati vengono archiviati in sistemi adeguatamente protetti, vengono gestiti da strumenti software di produttori certificati AgID

Marketplace per le PA e vengono trasmessi ad altri portali istituzionali attraverso canali sicuri di comunicazione e scambio dati.

	Descrizione del rischio	**Valutazione di rischio e contromisure da adottare**
Rischio 1	Perdita dei dati a seguito di hardware failure	Basso se l'Istituto è dotato di un sistema di disaster recovery Alto se l'Istituto non è dotato di un sistema di disaster recovery
Rischio 2	Furto di dati	Basso
Rischio 3	Intercettazione dei dati durante la trasmissione	Basso
Rischio 4	Accesso non autorizzato ai dati	Basso se l'istituto ha attivato la gestione di credenziali di accesso personali e ha correttamente sensibilizzato il personale

Soggetti coinvolti	**Modalità**
Direttore S.G.A.	Sensibilizzazione del personale amministrativo
Amministratore di Sistema	Verifica sussistenza delle misure adeguate di sicurezza tecnica e sistemistica

T04 - Finalità del trattamento: Gestione del Personale ATA

Categorie di interessati e categorie di dati personali

- personale ATA
- dati anagrafici del personale ATA;
- dati dei familiari del personale ATA;
- dati relativi alle assenze per malattia;
- dati relativi alle assenze per permessi familiari (congedi parentali) e per ragioni di studio/formazione/aggiornamento;
- dati relativi ai permessi per familiari portatori di handicap riconosciuto (Legge 104/92, L. 53/2000);
- dati relativi ai permessi per maternità/paternità; • dati relativi ai permessi sindacali/amministrativi;
- dati relativi alle ferie;
- dati relativi all'analisi delle situazioni di carriera (certificato di servizio e dichiarazione dei servizi prestati);
- contratti di lavoro;
- dati inerenti alla retribuzione/stipendi (dati bancari);
- titoli di studio;
- comunicazioni al personale necessarie alla gestione amministrativa del rapporto lavorativo (lettere, circolari, avvisi, ecc.); dati relativi alla gestione del contenzioso e dei procedimenti disciplinari;
- convocazioni in tribunale;
- dati relativi ai permessi per la donazione del sangue;
- dati relativi ai permessi non retribuiti per i supplenti;
- dati relativi ai permessi previsti dagli artt. 15, 16 DEL CCNL 29/11/07;
- dati necessari per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero della Pubblica Istruzione e dell'ordinamento scolastico;
- dati relativi alla partecipazione a scioperi;
- dati relativi alla partecipazione ad assemblee sindacali.

Natura dei dati

I dati trattati sono di natura comune, sensibile (dati idonei a rivelare le convinzioni religiose, filosofiche, sindacali, d'altro genere; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso; dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro; gestione del contenzioso e procedimenti disciplinari; dati idonei a rivelare la vita sessuale, esclusivamente in caso di rettificazione di attribuzione di sesso) e di carattere giudiziario (gestione del contenzioso e procedimenti disciplinari). I dati inerenti lo stato di salute sono trattati per: l'adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzioni del personale appartenente alle c.d. categorie

protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative pensionistiche, e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni e/o sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi per il personale e provvidenze, collegati a particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale;
I dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;
I dati sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;
I dati di carattere giudiziario sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato.
Le informazioni sulla vita sessuale possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso.

Ambito di comunicazione dei dati

- MIUR, Ufficio Scolastico Regionale, Ufficio Scolastico Provinciale;
- altri Istituti Scolastici, Enti di formazione;
- Ufficio di collocamento (dati dei supplenti, dati anagrafici, dati sul grado d'istruzione, durata della supplenza);
- Direzione Provinciale dei Servizi Vari (tesoreria), Ragioneria Provinciale dello Stato;
- INPS, INDIRE, Ministero dell'Economia;
- sindacati che con domanda motivata richiedano dati relativi ad attività esclusivamente connessa alle loro funzioni;
- assicurazioni private, INAIL, Revisore contabile, A.S.S.;
- musei, teatri, agenzie di viaggi, fondazioni;
- Comune, Provincia, Regione ed altri Enti Pubblici, anche per il personale assunto obbligatoriamente ai sensi della L. 68/1999;
- Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;
- Organi preposti al riconoscimento della causa di servizio/equo indennizzo» ai sensi del DPR 461/2001;
- Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (d.lg. n. 81/2008)
- Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del DPR. n. 1124/1965;
- Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
- Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;

- Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003 , n. 186;
- Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e DPR 20 febbraio 1998, n.38;
- Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413;
- MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335.
- Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, d.lg. n. 165/2001);
- Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D.Lgs. 30 marzo 2001, n. 165;
- Organi arbitrali: per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore;
- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di Giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati

- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS
- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è:

- esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
- esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso
-
-

Trattamento dei dati

- Data Controller: Direttore S.G.A.
- Data Processor: Assistenti amministrativi

Valutazione dei rischi

Il trattamento ha luogo all'interno degli uffici amministrativi. I dati vengono archiviati in sistemi adeguatamente protetti, vengono gestiti da strumenti software di produttori certificati AgID Marketplace per le PA e vengono trasmessi ad altri portali istituzionali attraverso canali sicuri di comunicazione e scambio dati.

	Descrizione del rischio	**Valutazione di rischio e contromisure da adottare**
Rischio 1	Perdita dei dati a seguito di hardware failure	Basso se l'Istituto è dotato di un sistema di disaster recovery Alto se l'Istituto non è dotato di un sistema di disaster recovery
Rischio 2	Furto di dati	Basso
Rischio 3	Intercettazione dei dati durante la trasmissione	Basso
Rischio 4	Accesso non autorizzato ai dati	Basso se l'istituto ha attivato la gestione di credenziali di accesso personali e ha correttamente sensibilizzato il personale

Soggetti coinvolti	**Modalità**
Direttore S.G.A.	Sensibilizzazione del personale amministrativo
Amministratore di Sistema	Verifica sussistenza delle misure adeguate di sicurezza tecnica e sistemistica

T05 - Finalità del trattamento: Gestione Alunni Diversamente Abili (Alunni "H", DVA, BES, etc)

Categorie di interessati e categorie di dati personali

Relativamente ad alunni portatori di handicap, l'Istituto tratta anche i seguenti dati:

- documentazione e lettere relative all'alunno;
- PEI Piano educativo individualizzato (si fa riferimento alla diagnosi);
- PDF profilo dinamico funzionale (si fa riferimento alla diagnosi);
- comunicazioni con famiglia e operatori sanitari;
- relazione finale;
- "certificazione" analisi mediche relativi all'Handicap;
- "diagnosi funzionale";
- valutazioni e verbali dell'alunno;
- accertamento Commissione Sanitaria ex DPCM 23/02/2006 n. 185;
- lettere e corrispondenza riservata con medici, Istituti specialistici.

Ambito di comunicazione dei dati

- Professionisti, strutture ospedaliere;
- ASS e Enti Locali per il funzionamento dei Gruppi di Lavoro di istituto per l'Handicap e per la predisposizione e la verifica del Piano Educativo Individuale ai sensi della Legge 5 febbraio 1992, n. 104;
- Cooperative private di sostegno agli allievi "H";
- Enti Pubblici.

Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS
- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è:

- esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
- esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso

Trattamento dei dati

Data Controller: Direttore S.G.A.
Data Processor: Assistenti amministrativi

Valutazione dei rischi

Il trattamento ha luogo all'interno degli uffici amministrativi. I dati vengono archiviati in sistemi adeguatamente protetti, vengono gestiti da strumenti software di produttori certificati AgID Marketplace per le PA e vengono trasmessi ad altri portali istituzionali attraverso canali sicuri di comunicazione e scambio dati.

	Descrizione del rischio	**Valutazione di rischio e contromisure da adottare**
Rischio 1	Perdita dei dati a seguito di hardware failure	Basso se l'Istituto è dotato di un sistema di disaster recovery Alto se l'Istituto non è dotato di un sistema di disaster recovery
Rischio 2	Furto di dati	Basso
Rischio 3	Intercettazione dei dati durante la trasmissione	Basso
Rischio 4	Accesso non autorizzato ai dati	Basso se l'istituto ha attivato la gestione di credenziali di accesso personali e ha correttamente sensibilizzato il personale

Soggetti coinvolti	**Modalità**
Direttore S.G.A.	Sensibilizzazione del personale amministrativo
Amministratore di Sistema	Verifica sussistenza delle misure adeguate di sicurezza tecnica e sistemistica

T06 - Finalità del trattamento: Gestione Fornitori di Beni e Servizi

Categorie di interessati e categorie di dati personali

- dati anagrafici fornitori: nome, cognome, codice fiscale, indirizzo, P.IVA, denominazione/ragione sociale, sede legale/amministrativa, coordinate bancarie, referenti interni, telefono, indirizzo e-mail, ecc;
- documenti contabili/fiscali;
- preventivi, offerte;
- comunicazioni tra Istituto e fornitori;
- contratti e convenzioni.

Natura dei dati

I dati trattati sono di natura comune.

Ambito di comunicazione dei dati

- Ufficio Scolastico Provinciale, MIUR, Ministero delle Finanze;
- altri istituti scolastici;
- Direzione provinciale dei Servizi Vari (Tesoreria);
- Comune, Provincia, Regione ed altri Enti Pubblici;
- Revisore dei conti;
- Fondazioni, Istituti Bancari, Assicurazioni;
- Professionisti: (Studi legali, Arbitri, ecc.).

Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS
- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è:

- esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
- esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso

Trattamento dei dati

Data Controller: Direttore S.G.A.
Data Processor: Assistenti amministrativi

Valutazione dei rischi

Il trattamento ha luogo all'interno degli uffici amministrativi. I dati vengono archiviati in sistemi adeguatamente protetti, vengono gestiti da strumenti software di produttori certificati AgID Marketplace per le PA e vengono trasmessi ad altri portali istituzionali attraverso canali sicuri di comunicazione e scambio dati.

	Descrizione del rischio	**Valutazione di rischio e contromisure da adottare**
Rischio 1	Perdita dei dati a seguito di hardware failure	Basso se l'Istituto è dotato di un sistema di disaster recovery Alto se l'Istituto non è dotato di un sistema di disaster recovery
Rischio 2	Furto di dati	Basso
Rischio 3	Intercettazione dei dati durante la trasmissione	Basso
Rischio 4	Accesso non autorizzato ai dati	Basso se l'istituto ha attivato la gestione di credenziali di accesso personali e ha correttamente sensibilizzato il personale

Soggetti coinvolti	**Modalità**
Direttore S.G.A.	Sensibilizzazione del personale amministrativo
Amministratore di Sistema	Verifica sussistenza delle misure adeguate di sicurezza tecnica e sistemistica

T07 - Finalità del trattamento: Gestione del Registro Elettronico

Categorie di interessati e categorie di dati personali

- alunni, docenti;
- dati anagrafici degli alunni e dei docenti: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.;
- dati personali dei familiari degli alunni;
- dati relativi alle assenze degli alunni;
- valutazioni dell'alunno;
- diplomi ed attestati;
- scelta relativa all'ora di religione;
- curriculum scolastico (promozioni, bocciature);
- comunicazioni tra scuola e studente/famiglia dello studente;
- dati relativi ad eventuali handicap;
- lettere e comunicazioni alle famiglie;
- personale docente a tempo determinato ed indeterminato;
- dati relativi alla partecipazione a scioperi;
- dati relativi alla partecipazione ad assemblee sindacali.

Natura dei dati

I dati trattati sono di natura comune, sensibile (dati idonei a rivelare l'origine razziale o etnica, per favorire l'integrazione degli alunni stranieri; dati idonei a rivelare le convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento; dati idonei a rivelare le convinzioni filosofiche, politiche, d'altro genere, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei familiari; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso, per assicurare l'erogazione del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate a quelle motorie e sportive, alle visite guidate e ai viaggi d'istruzione, all'erogazione del servizio mensa) e dati a carattere giudiziario (nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno e/o della famiglia dell'alunno, oppure per la gestione del contenzioso con le famiglie degli alunni).

Ambito di comunicazione dei dati

I dati rimangono all'interno della piattaforma Registro Elettronico. Non sono previste comunicazioni di dati all'esterno.

Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- acquisizione della documentazione redatta dal fornitore del servizio Registro Elettronico, relativa alle misure tecniche ed organizzative di sicurezza implementate dal fornitore del servizio

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è:

- esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
- esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso

Trattamento dei dati

Data Controller: Direttore S.G.A.
Data Controller: Titolare del Trattamento
Data Processor: Assistenti amministrativi
Data Processor: Personale docente

Valutazione dei rischi

Il trattamento ha luogo sia all'interno dell'istituto scolastico sia all'esterno. I dati vengono archiviati in sistemi adeguatamente protetti, vengono gestiti da strumenti software di produttori certificati AgID Marketplace per le PA e vengono trasmessi ad altri portali istituzionali attraverso canali sicuri di comunicazione e scambio dati.
I terminali di accesso al sistema possono non essere tutti adeguatamente protetti e non sono tutti controllabili, dal momento che i docenti possono accedere al sistema in Cloud da casa con i propri strumenti personali.

	Descrizione del rischio	**Valutazione di rischio e contromisure da adottare**
Rischio 1	Perdita dei dati a seguito di hardware failure	Basso
Rischio 2	Furto di dati	Medio. Occorre sensibilizzare il personale docente sull'importanza di un corretto utilizzo dello strumento, delle modalità corrette di disconnessione e di una corretta gestione delle credenziali di accesso
Rischio 3	Intercettazione dei dati durante la trasmissione	Basso
Rischio 4	Accesso non autorizzato ai dati	Alto. Occorre sensibilizzare il personale docente sull'importanza di un corretto utilizzo dello strumento, delle modalità corrette di disconnessione e di una corretta gestione delle credenziali di accesso
Rischio 5	Caduta del servizio a causa di attacchi DoS	Basso. I sistemi in Cloud sono esposti al rischio di attacchi DoS. Il fornitore del servizio ha specificato nel proprio manuale tecnico le modallità di protezione e contenimento degli attacchi informatici.

Soggetti coinvolti	Modalità
Direttore S.G.A.	Sensibilizzazione del personale amministrativo
Amministratore di Sistema	Verifica sussistenza delle misure adeguate di sicurezza tecnica e sistemistica
Personale docente	Sensibilizzazione del personale docente

T08 - Finalità del trattamento: Gestione del Sito Web istituzionale

Categorie di interessati e categorie di dati personali

- alunni, docenti;
- dati anagrafici degli alunni e dei docenti: nome, cognome, indirizzo email

Natura dei dati

I dati trattati sono di natura comune,

Ambito di comunicazione dei dati

I dati rimangono all'interno della piattaforma del sito web istituzionale. Non sono previste comunicazioni di dati all'esterno.

Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- designazione del Responsabile della protezione dei dati

- individuazione degli eventi che possono compromettere la sicurezza
- acquisizione della documentazione redatta dal fornitore del servizio di Hosting, relativa alle misure tecniche ed organizzative di sicurezza implementate dal fornitore del servizio

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è:

- esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
- esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso

Trattamento dei dati

Data Controller: Direttore S.G.A.
Data Controller: Titolare del Trattamento
Data Processor: Assistenti amministrativi
Data Processor: Amministratore del sito web

Valutazione dei rischi

Il trattamento ha luogo sia all'interno dell'istituto scolastico sia all'esterno. I dati vengono archiviati in sistemi adeguatamente protetti, vengono gestiti da strumenti software di produttori certificati AgID Marketplace per le PA e vengono trasmessi ad altri portali istituzionali attraverso canali sicuri di comunicazione e scambio dati.
I terminali di accesso al sistema possono non essere tutti adeguatamente protetti e non sono tutti controllabili, dal momento che i docenti possono accedere al sistema in Cloud da casa con i propri strumenti personali.

	Descrizione del rischio	**Valutazione di rischio e contromisure da adottare**
Rischio 1	Perdita dei dati a seguito di hardware failure	Basso

Rischio 2	Furto di dati	Medio. Occorre sensibilizzare il personale docente sull'importanza di un corretto utilizzo dello strumento, delle modalità corrette di disconnessione e di una corretta gestione delle credenziali di accesso
Rischio 3	Intercettazione dei dati durante la trasmissione	Basso
Rischio 4	Accesso non autorizzato ai dati	Alto. Occorre sensibilizzare il personale docente sull'importanza di un corretto utilizzo dello strumento, delle modalità corrette di disconnessione e di una corretta gestione delle credenziali di accesso
Rischio 5	Caduta del servizio a causa di attacchi DoS	Basso. I sistemi in Cloud sono esposti al rischio di attacchi DoS. Il fornitore del servizio ha specificato nel proprio manuale tecnico le modallità di protezione e contenimento degli attacchi informatici.

Soggetti coinvolti	**Modalità**
Direttore S.G.A.	Sensibilizzazione del personale amministrativo
Amministratore di Sistema	Verifica sussistenza delle misure adeguate di sicurezza tecnica e sistemistica
Personale docente	Sensibilizzazione del personale docente
Amministratore del sito web	Verifica corretto aggiornamento dei servizi del sito web, del motore CMS, dei plugin e dei sistemi di protezione e backup del sito

T09 - Finalità del trattamento: Gestione del Processo di Dematerializzazione

Categorie di interessati e categorie di dati personali

- Alunni, docenti, personale ATA, fornitori, enti;
- alunni ed ex-alunni
- dati anagrafici degli alunni: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.;
- dati personali dei familiari degli alunni;
- dati relativi alle assenze;
- certificati medici;
- valutazione dell'alunno;
- diplomi ed attestati;
- scelta relativa all'ora di religione;
- curriculum scolastico (promozioni, bocciature);
- comunicazioni tra scuola e studente/famiglia dello studente;
- tasse scolastiche (esoneri); dati relativi alla gestione del contenzioso;
- dati relativi ad eventuali handicap;
- dati comunicati da Tribunali dei minorenni, Tribunali, Assistenti sociali;
- lettere e comunicazioni alle famiglie;
- fotografie, riprese audio-video (eventuali);
- Relativamente ad alunni portatori di handicap, l'Istituto tratta anche i seguenti dati:
- documentazione e lettere relative all'alunno;
- PEI Piano educativo individualizzato (si fa riferimento alla diagnosi);
- PDF profilo dinamico funzionale (si fa riferimento alla diagnosi);
- comunicazioni con famiglia e operatori sanitari;
- relazione finale;
- "certificazione" analisi mediche relativi all'Handicap;
- "diagnosi funzionale";
- valutazioni e verbali dell'alunno;
- accertamento Commissione Sanitaria ex DPCM 23/02/2006 n. 185;
- lettere e corrispondenza riservata con medici, Istituti specialistici;
- personale docente a tempo determinato ed indeterminato;
- dati anagrafici degli insegnanti a tempo indeterminato, insegnanti a tempo determinato, insegnanti esterni incaricati di funzioni nella scuola: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.;
- dati dei familiari degli insegnanti a tempo indeterminato, insegnanti a tempo determinato, insegnanti esterni incaricati di funzioni nella scuola;
- dati relativi alle assenze per malattia;
- dati relativi alle assenze per permessi familiari (congedi parentali) e per ragioni di studio/formazione/aggiornamento;

- dati relativi ai permessi per familiari portatori di handicap riconosciuto (Legge 104/92, L. 53/2000);
- dati relativi ai permessi per maternità/paternità;
- dati relativi ai permessi sindacali/amministrativi;
- dati relativi alle ferie;
- dati relativi all'analisi delle situazioni di carriera (certificato di servizio e dichiarazione dei servizi prestati);
- contratti di lavoro;
- dati inerenti alla retribuzione/stipendi (dati bancari);
- titoli di studio, dati sul grado di istruzione;
- dati relativi alle altre attività eventualmente svolte dal personale docente;
- comunicazioni al personale necessarie alla gestione amministrativa del rapporto lavorativo (lettere, circolari, avvisi, ecc.);
- dati relativi alla gestione del contenzioso e dei procedimenti disciplinari;
- convocazioni in tribunale;
- dati relativi ai permessi per la donazione del sangue;
- dati relativi ai permessi non retribuiti per i supplenti;
- dati relativi ai permessi previsti dagli artt. 15, 16 DEL CCNL 29/11/07;
- dati necessari per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero della Pubblica Istruzione e dell'ordinamento scolastico;
- dati relativi alla partecipazione a scioperi;
- dati relativi alla partecipazione ad assemblee sindacali;
- personale ATA
- dati anagrafici del personale ATA;
- dati dei familiari del personale ATA;
- dati relativi alle assenze per malattia;
- dati relativi alle assenze per permessi familiari (congedi parentali) e per ragioni di studio/formazione/aggiornamento;
- dati relativi ai permessi per familiari portatori di handicap riconosciuto (Legge 104/92, L. 53/2000);
- dati relativi ai permessi per maternità/paternità;
- dati relativi ai permessi sindacali/amministrativi;
- dati relativi alle ferie;
- dati relativi all'analisi delle situazioni di carriera (certificato di servizio e dichiarazione dei servizi prestati);
- contratti di lavoro;
- dati inerenti alla retribuzione/stipendi (dati bancari);
- titoli di studio;
- comunicazioni al personale necessarie alla gestione amministrativa del rapporto lavorativo (lettere, circolari, avvisi, ecc.); dati relativi alla gestione del contenzioso e dei procedimenti disciplinari;
- convocazioni in tribunale;
- dati relativi ai permessi per la donazione del sangue;
- dati relativi ai permessi non retribuiti per i supplenti;
- dati relativi ai permessi previsti dagli artt. 15, 16 DEL CCNL 29/11/07;

- dati necessari per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero della Pubblica Istruzione e dell'ordinamento scolastico;
- dati relativi alla partecipazione a scioperi;
- dati relativi alla partecipazione ad assemblee sindacali;
- dati anagrafici fornitori: nome, cognome, codice fiscale, indirizzo, P.IVA, denominazione/ragione sociale, sede legale/amministrativa, coordinate bancarie, referenti interni, telefono, indirizzo e-mail, ecc;
- documenti contabili/fiscali;
- preventivi, offerte;
- comunicazioni tra Istituto e fornitori;
- contratti e convenzioni.

Natura dei dati

I dati trattati sono di natura comune, sensibile (dati idonei a rivelare l'origine razziale o etnica, per favorire l'integrazione degli alunni stranieri; dati idonei a rivelare le convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento; dati idonei a rivelare le convinzioni filosofiche, politiche, d'altro genere, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei familiari; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso, per assicurare l'erogazione del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate a quelle motorie e sportive, alle visite guidate e ai viaggi d'istruzione, all'erogazione del servizio mensa) e dati a carattere giudiziario (nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno e/o della famiglia dell'alunno, oppure per la gestione del contenzioso con le famiglie degli alunni).

Ambito di comunicazione dei dati

- Ufficio Scolastico Provinciale, MIUR, Ministero delle Finanze;
- altri istituti scolastici;
- Direzione provinciale dei Servizi Vari (Tesoreria);
- Comune, Provincia, Regione ed altri Enti Pubblici;
- Revisore dei conti;
- Fondazioni, Istituti Bancari, Assicurazioni;
- Professionisti: (Studi legali, Arbitri, ecc.).

Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- acquisizione della documentazione redatta dal fornitore del servizio di dematerializzazione Segreteria Digitale, relativa alle misure tecniche ed organizzative di sicurezza implementate dal fornitore del servizio

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è:

- esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale

- esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso

Trattamento dei dati

Data Controller: Direttore S.G.A.
Data Processor: Assistenti amministrativi

Valutazione dei rischi

Il trattamento ha luogo sia all'interno dell'istituto scolastico sia all'esterno. I dati vengono archiviati in sistemi adeguatamente protetti, vengono gestiti da strumenti software di produttori certificati AgID Marketplace per le PA e vengono trasmessi ad altri portali istituzionali attraverso canali sicuri di comunicazione e scambio dati.
I terminali di accesso al sistema possono non essere tutti adeguatamente protetti e non sono tutti controllabili, dal momento che è possibile accedere al sistema in Cloud da casa con i propri strumenti personali.

	Descrizione del rischio	**Valutazione di rischio e contromisure da adottare**
Rischio 1	Perdita dei dati a seguito di hardware failure	Basso
Rischio 2	Furto di dati	Medio. Occorre sensibilizzare il personale sull'importanza di un corretto utilizzo dello strumento, delle modalità corrette di disconnessione e di una corretta gestione delle credenziali di accesso
Rischio 3	Intercettazione dei dati durante la trasmissione	Basso
Rischio 4	Accesso non autorizzato ai dati	Alto. Occorre sensibilizzare il personale sull'importanza di un corretto utilizzo dello strumento, delle modalità corrette di disconnessione e di una corretta gestione delle credenziali di accesso
Rischio 5	Caduta del servizio a causa di attacchi DoS	Basso. I sistemi in Cloud sono esposti al rischio di attacchi DoS. Il fornitore del servizio ha specificato nel proprio manuale tecnico le modallità di protezione e contenimento degli attacchi informatici.

Soggetti coinvolti	**Modalità**
Direttore S.G.A.	Sensibilizzazione del personale amministrativo
Amministratore di Sistema	Verifica sussistenza delle misure adeguate di sicurezza tecnica e sistemistica

T10 - Finalità del trattamento: Attivazione della modalità di Didattica a Distanza

Categorie di interessati e categorie di dati personali

- alunni, docenti;
- dati anagrafici degli alunni e dei docenti: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.;
- dati personali dei familiari degli alunni;
- dati relativi alle assenze degli alunni;
- valutazioni dell'alunno;
- diplomi ed attestati;
- scelta relativa all'ora di religione;
- curriculum scolastico (promozioni, bocciature);
- comunicazioni tra scuola e studente/famiglia dello studente;
- dati relativi ad eventuali handicap;
- lettere e comunicazioni alle famiglie;
- personale docente a tempo determinato ed indeterminato;

Natura dei dati

I dati trattati sono di natura comune, sensibile (dati idonei a rivelare l'origine razziale o etnica, per favorire l'integrazione degli alunni stranieri; dati idonei a rivelare le convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento; dati idonei a rivelare le convinzioni filosofiche, politiche, d'altro genere, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei familiari; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso, per assicurare l'erogazione del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate a quelle motorie e sportive, alle visite guidate e ai viaggi d'istruzione, all'erogazione del servizio mensa) e dati a carattere giudiziario (nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno e/o della famiglia dell'alunno, oppure per la gestione del contenzioso con le famiglie degli alunni).

Ambito di comunicazione dei dati

I dati rimangono all'interno della piattaforma utilizzata per l'erogazione della modalità di Didattica a Distanza (DaD). Non sono previste comunicazioni di dati all'esterno.

Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea o rispondente ai requisiti fissati dal Regolamento Europeo 679/2016 GDPR.

Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- acquisizione della documentazione redatta dal fornitore del servizio di Didattica a Distanza, relativa alle misure tecniche ed organizzative di sicurezza implementate dal fornitore del servizio

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è:

- esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale

- espletamento di quanto previsto dal Decreto Legge n. 6 del 23/02/2020 e successivi Decreti integrativi del Presidente del Consiglio dei Ministri

Trattamento dei dati

Data Controller: Direttore S.G.A.
Data Controller: Titolare del Trattamento
Data Processor: Assistenti amministrativi
Data Processor: Personale docente

Valutazione dei rischi

Il trattamento ha luogo sia all'interno dell'istituto scolastico sia all'esterno. I dati vengono archiviati in sistemi adeguatamente protetti, vengono gestiti da strumenti software di produttori certificati AgID Marketplace per le PA e vengono trasmessi ad altri portali istituzionali attraverso canali sicuri di comunicazione e scambio dati.
I terminali di accesso al sistema possono non essere tutti adeguatamente protetti e non sono tutti controllabili, dal momento che i docenti possono accedere al sistema in Cloud da casa con i propri strumenti personali.

	Descrizione del rischio	**Valutazione di rischio e contromisure da adottare**
Rischio 1	Perdita dei dati a seguito di hardware failure	Basso. Il fornitore del servizio ha specificato nel proprio manuale tecnico le modalità di protezione e ridondanza dei dati
Rischio 2	Furto di dati	Medio. Occorre sensibilizzare il personale docente sull'importanza di un corretto utilizzo dello strumento, delle modalità corrette di disconnessione e di una corretta gestione delle credenziali di accesso
Rischio 3	Intercettazione dei dati durante la trasmissione	Basso
Rischio 4	Accesso non autorizzato ai dati	Alto. Occorre sensibilizzare il personale docente sull'importanza di un corretto utilizzo dello strumento, delle modalità corrette di disconnessione e di una corretta gestione delle credenziali di accesso Occorre altresì utilizzare piattaforme con privacy policies conformi a quanto prescritto dal GDPR e possibilmente elencate tra quelle autorizzate dal MIUR

Rischio 5	Caduta del servizio a causa di attacchi DoS	Basso. I sistemi in Cloud sono esposti al rischio di attacchi DoS. Il fornitore del servizio ha specificato nel proprio manuale tecnico le modalità di protezione e contenimento degli attacchi informatici.

Soggetti coinvolti	**Modalità**
Direttore S.G.A.	Sensibilizzazione del personale amministrativo
Amministratore di Sistema	Verifica sussistenza delle misure adeguate di sicurezza tecnica e sistemistica
Personale docente	Sensibilizzazione del personale docente

T11 - Finalità del trattamento: Attivazione della piattaforma Cloud Google Workspace

A seguito del cambiamento delle proprie policies di trattamento e gestione dei dati, allo scopo di uniformarsi alle direttive contenute nel Regolamento Europeo 679/2016 GDPR, Google ha rilasciato una propria DPIA, consultabile al seguente URL:
https://cloud.google.com/privacy/data-protection-impact-assessment
Riportiamo qui di seguito l'analisi del trattamento e la valutazione dei rischi condotta da Google:

DPIA Criteria	Relevant Information about the Cloud Services
A systematic description of the envisaged processing operations	
nature, scope and context of processing	If the Customer is the relevant controller of Customer Personal Data, then that Customer is responsible for completing any DPIA required under the EU GDPR. Google will act as the Customer's processor of Customer Personal Data, processing that data strictly as instructed by the Customer. These roles are described in the DPA and the DPST. The Cloud Services cover a wide range of potential uses and are highly configurable: Google Workspace (including Google Workspace for Education) services offer extensive productivity and collaboration tools; and Google Cloud services comprise over 150 cloud computing, data analytics and machine learning products. As a controller of Customer Personal Data processed via the relevant Cloud Services, the Customer is responsible for determining the nature, scope and context of the processing of that data. This will include determining the following, for example: the nature of the Customer Personal Data; the volume and variety of the Customer Personal Data, number of data subjects involved, etc.
categories of personal data processed	As set out in Appendix 1 of the DPA and DPST, the 'categories of data' processed via the Cloud Services will encompass any data relating to individuals that is provided to Google, via the Cloud Services, by (or at the direction of) Customer or its End Users, including, in the case of Google Workspace, any data submitted, stored, sent or received via Google Workspace. Depending on the Customer's envisaged use of the Cloud Services, these categories may include any special categories of personal data, i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data; biometric data (where this is used for identification purposes); or data concerning health, sex life or sexual orientation. Further categories of personal data processed may also be relevant (e.g. identification data, location data, or behavioural preferences), again depending on the Customer's envisaged use of the Cloud Services.

recipients of the personal data	The Customer, as controller of Customer Personal Data, is responsible for determining the third parties with whom that data is shared. Google, as a processor of that data, is a recipient of it. Google, as processor, also engages Subprocessors authorised by the Customer under the DPA and/or DPST to perform limited activities in connection with the Cloud Services. The Subprocessors currently engaged by Google are listed here (for Google Workspace, including Google Workspace for Education) and here (for Google Cloud). Google's commitments For each Subprocessor, Google commits in the DPA and DPST to: • ensure that the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Cloud Contract (including the DPA and/or DPST, as applicable); • ensure that, if the processing of Customer Personal Data is subject to the EU GDPR (or any other European Data Protection Law), then the data protection obligations described in the DPA and/or DPST (as applicable) are imposed on the Subprocessor; and • provide each Customer with advance notice before a new Subprocessor starts processing any Customer Data, including in this notice the Subprocessor's name and location, and the activities it will perform. Activities Subprocessors are engaged to perform: • TSS; • Data Center Operations; and • Service Maintenance. Each activity is described in more detail in our Google Workspace Subprocessor list and Google Cloud Subprocessor list. Access to Customer Data Our Google Workspace Subprocessor list and Google Cloud Subprocessor list describe each Subprocessor's access to Customer Data based on the activity they are engaged to perform for the respective Cloud Services.

period for which the personal data will be stored	As set out in Appendix 1 of the DPA and/or DPST (as applicable), Google will process the Customer Data for the Term plus the period from the end of the Term until deletion of all Customer Data by Google in accordance with the DPA and/or DPST. Google will enable the Customer to delete Customer Data during the Term in a manner consistent with the functionality of the relevant Cloud Services. If the Customer wishes to retain any Customer Data after the end of the Term, it may instruct Google to return that data during the Term, and the Customer instructs Google to delete all remaining Customer Data (including existing copies) from Google's systems at the end of the Term in accordance with applicable law. After a recovery period of up to 30 days from that date, Google will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage. For more information about retention and deletion for: • Google Workspace (including Google Workspace for Education), see our help center articles on Delete or remove a user from your organization and Delete your organization's Google Account • Google Cloud: See our Data deletion on Google Cloud page. The Customer, as controller of Customer Personal Data, is responsible for copies of that data it may choose to store outside Google's or its Subprocessors' systems.
a functional description of the processing operation(s)	The Google Workspace (including Google Workspace for Education) services are productivity and collaboration tools and are described in the Google Workspace Services Summary. For more information about service features, see here for Google Workspace and here for Google Workspace for Education. The Google Cloud services comprise over 150 cloud computing, data analytics and machine learning products and are described in the Google Cloud Services Summary. For more information about service features, see here.

the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels)	Google may store and process Customer Data where Google or its Subprocessors maintain facilities. For the Google Workspace (including Google Workspace for Education) services: • information about the locations of Google's facilities is available here; and • information about the locations of Subprocessors' facilities is available here. For the Google Cloud services: • information about the locations of Google's facilities is available here; and • information about the locations of Subprocessors' facilities is available here. More information about relevant infrastructure (including hardware and networks) used in the performance of Cloud Services (including for the processing of Customer Data) is available in our Security Infrastructure Design Overview, as well as: • for Google Workspace (including Google Workspace for Education), in the Google Workspace Security whitepaper; and • for Google Cloud, in the Google security overview.
compliance with approved codes of conduct is taken into account	Google adheres to the EU GDPR Cloud Code of Conduct (CoC) with respect to the Cloud Services. This CoC is a mechanism for cloud providers to demonstrate how they offer sufficient guarantees to implement appropriate technical and organisational measures as processors under the EU GDPR.
The purposes of the processing, including, where applicable, the legitimate interest pursued by the controller	
purposes of the processing	The Customer, as controller of Customer Personal Data, instructs Google to process that data only in accordance with applicable law: to provide, secure, and monitor the Services and TSS; as further specified via the Customer's use of the relevant Cloud Services and TSS; and as documented in the relevant Cloud Contract, including the DPA and/or DPST (as applicable). Google will comply with the Customer's instructions under the DPA and/or DPST (unless prohibited by European Law) with respect to such processing.
An assessment of the necessity and proportionality of the processing operations in relation to the purposes	

specified, explicit and legitimate purpose	The Customer, as controller of Customer Personal Data, is responsible for complying with the 'purpose limitation' principle (under Article 5 of the EU GDPR) with respect to any such data processed via the Cloud Services. As described in the DPA and/or DPST (as applicable), the Customer instructs Google to process Customer Personal Data only in accordance with applicable law: to provide, secure, and monitor the Services and TSS; as further specified via the Customer's use of the Services and TSS; and as documented in the Agreement, including the DPA and/or DPST. Google will comply with the Customer's instructions under the DPA and/or DPST (unless prohibited by European Law) with respect to such processing.
lawfulness of processing	The Customer, as controller of Customer Personal Data, is responsible for determining the lawfulness of its processing via the Cloud Services. As described in the DPA and/or DPST (as applicable), the Customer instructs Google to process Customer Personal Data only in accordance with applicable law for the purposes specified in the DPA and/or the DPST. Google will comply with the Customer's instructions under the DPA and/or DPST (unless prohibited by European Law) with respect to such processing. Both the Customer and Google also commit, in the DPA and/or DPST, to complying with their respective obligations under the EU GDPR (and any other European Data Protection Law).
adequate, relevant and limited to what is necessary	The Customer, as controller of Customer Personal Data, is responsible for complying with the 'data minimisation' principle (under Article 5 of the EU GDPR) when any such data is processed via the Cloud Services. As described in the DPA and/or DPST (as applicable), the Customer instructs Google to process Customer Personal Data only in accordance with applicable law: to provide, secure, and monitor the Services and TSS; as further specified via the Customer's use of the Services and TSS; and as documented in the Agreement, including the DPA and/or DPST. Google will comply with the Customer's instructions under the DPA and/or DPST (unless prohibited by European Law) with respect to such processing.
storage limitation	The Customer, as controller of Customer Personal Data, is responsible for complying with the 'storage limitation' principle (under Article 5 of the EU GDPR) when any such data is processed via the Cloud Services. Please see the "period for which the personal data will be stored" section above for relevant information about Google's retention and deletion commitments with respect to the Cloud Services.
information provided to the data subject	The Customer, as controller of Customer Personal Data, is responsible for complying with Articles 12-14 of the EU GDPR when any such data is processed via the Cloud Services.

measures contributing to data subject rights	The Customer, as controller of Customer Personal Data, is responsible under Chapter III of the EU GDPR for responding to requests from data subjects to exercise their rights relating to that data under Chapter III. To help the Customer fulfill these obligations, Google commits in the DPA and DPST to enable the Customer during the Term, in a manner consistent with the functionality of the Cloud Services, to delete, access, rectify and restrict processing of Customer Data (including via the deletion functionality provided by Google) and to export Customer Data. The Customer can use the Admin Console and other functionality of the Cloud Services to access, rectify, restrict the processing of, or delete any Customer Personal Data. Additionally, if during the Term Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies the Customer, Google will: (a) advise the data subject to submit their request to the Customer; (b) promptly notify the Customer; and (c) not otherwise respond to that data subject's request without authorization from the Customer. The Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Cloud Services. Specifically for Google Workspace (including Google Workspace for Education) services, the Google Workspace Data Subject Requests (DSR) Guide provides more information on how a Google Workspace Administrator can use Google Workspace Admin Console features to help the Customer fulfill its obligations to respond to requests from data subjects.
relationships with processor	The DPA and DPST bind Google, as the Customer's processor of Customer Personal Data, and otherwise reflect the contracting requirements under Article 28 of the EU GDPR.

safeguards surrounding international transfer(s)	The Customer and Google, as controller and processor respectively of Customer Personal Data, are responsible for ensuring that any transfers of such data to third countries comply with the requirements of Chapter V of the EU GDPR. To legitimize any transfers of Customer Personal Data to non-adequate third countries, Google relies on the new EU SCCs, as described in the DPA and/or DPST (as applicable) and in more detail in our Google Cloud's Approach to the New EU Standard Contractual Clauses whitepaper. In particular, you may wish to review the section titled "Google Cloud's New Approach to SCCs" to understand which SCC module(s) are applicable with respect to relevant transfers of Customer Personal Data. We also provide information about our technical, legal, and organisational safeguards for Google Workspace (including Google Workspace for Education) in our Safeguards for International Data Transfers with Google Workspace and Workspace for Education whitepaper and our Safeguards for International Data Transfers with Google Cloud whitepaper . These whitepapers include information about United States laws and their applicability to the Cloud Services to help customers with any risk assessments they may need to complete in light of the Court of Justice of the European Union's ruling known as "Schrems II".
prior consultation with the supervisory authority	The Customer, as controller of Customer Personal Data, is responsible for complying with Article 36 of the EU GDPR with respect to prior consultations with any relevant supervisory authority. To support those consultations, the Customer may refer to any information contained in this Resource Center.
An assessment of the risks to the rights and freedoms of data subjects	
origin, nature, particularity and severity of the risks	The Customer, as controller of Customer Personal Data, is responsible for determining and assessing the risks to the rights and freedoms of data subjects in connection with the Customer's envisaged implementation and operation of the Cloud Services. For more information about privacy and security best practices when implementing and using the Cloud Services, see: • Our data protection implementation guides for Google Workspace and Google Workspace for Education • Our security best practices center, which contains various security-focused resources for the Cloud Services
The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data	

measures envisaged to treat the risks are determined	The Customer and Google, as controller and processor respectively of Customer Personal Data, are responsible under Article 32 of the EU GDPR for implementing appropriate technical and organisational measures to secure that data, as appropriate to the risks involved. Under the DPA and/or DPST (as applicable), the Customer agrees that the relevant Cloud Services, the Security Measures implemented and maintained by Google, the Additional Security Controls and Google's commitments under the DPA and/or DPST provide an appropriate level of security in light of those risks. Security measures As described in our Security Infrastructure Design Overview, Google has a global scale technical infrastructure designed to provide security through Google's entire information processing life cycle. Specifically, this infrastructure is designed to provide secure deployment of the Cloud Services, secure storage of Customer Data, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators. More information about the specific technical and organisational measures maintained by Google with respect to: • Google Workspace (including Google Workspace for Education) is set out in the Google Workspace Security Whitepaper; and • Google Cloud is set out in the Google Security Overview. Additional extensive resources concerning Google's technical and organizational security measures for the Cloud Services are available at our Security Best Practices Center and Privacy Resource Center. Google also offers optional Additional Security Controls to help Cloud Services customers meet their security and compliance needs. These controls are described in the resources available at our Security Best Practices Center and Privacy Resource Center mentioned above. Standards and best practices The Cloud Services regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations, and audit reports to demonstrate compliance. Customers can directly access and download various certifications (including ISO 27001, 27017, 27018 and 27701), audit reports (including SOC 1, 2 and 3) and other relevant resources via our Compliance Reports Manager. Additionally, as mentioned above, Google adheres to the EU GDPR Cloud Code of Conduct (CoC) with respect to the Cloud Services. Contractual security commitments Under the DPA and DPST, Google commits to implement and maintain technical and organisational measures to protect Customer Data against accidental or

	unlawful destruction, loss, alteration, unauthorised disclosure or access. These measures are described in Appendix 2 of the DPA and DPST. Organisational safeguards Our Transparency Report discloses, where permitted by applicable law, the number of requests made by law enforcement agencies and government bodies for Enterprise Cloud customer information. Google will follow the processes described in the Government Requests for Cloud Customer Data whitepaper with respect to any such requests.

Informativa

L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016. E' fornita Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato).

Base giuridica

E' la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.
La base giuridica del trattamento è:

- esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
- espletamento di quanto previsto dal Decreto Legge n. 6 del 23/02/2020 e successivi Decreti integrativi del Presidente del Consiglio dei Ministri

Trattamento dei dati

Data Controller: Direttore S.G.A.
Data Controller: Titolare del Trattamento
Data Processor: Assistenti amministrativi
Data Processor: Personale docente

Definizioni

Ai fini del presente documento, ai sensi dell'art. 4 del Regolamento UE 679/2016, si intende per:

a) «**Dato personale**»: qualsiasi informazione riguardante una **persona fisica identificata o identificabile** («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) «**Trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c) «**Data Controller**»: la figura che mette in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato

d) «**Profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

e) «**Titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

f) «**Responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

g) «**Destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

h) «**Terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

i) **«Pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e

soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

j) «**Consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

k) «**Dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

l) «**Dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

m) **«Dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

n) **«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;

o) **«Archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

p) «**Trattamento transfrontaliero**»:

1. trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
2. trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

Protezione dei dati

Di seguito si riporta lo schema di sintesi delle misure di sicurezza applicabili, una breve descrizione delle stesse e la modalità di trattamento a cui si riferisce.

Misure specifiche per la protezione dei dati

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
MPD-1	**Minimizzazione della quantità di dati personali**	Misure volte a gestire solo dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.	✓	✓	✓
MPD-2	**Partizionamento dei dati**	Misure volte a separare le aree di archiviazione dei dati personali trattati al fine di ridurre la possibilità che i dati possano essere correlati e compromessi, ad esempio attraverso la creazione di cartelle di rete condivise distinte per tipologia di dati personali o l'archiviazione di documentazione cartacea in faldoni o archivi separati.	✓	✓	✓
MPD-3	**Cifratura**	Misure volte ad assicurare la riservatezza dei dati personali archiviati (in database, documenti e archivi elettronici, etc.) o trasmessi attraverso le reti (ad es., VPN, HTTPS, TLS, etc.) e per gestire chiavi crittografiche.	✓		✓
MPD-4	**Pseudo-nimizzazione**	Misura tecnica volta a rendere anonimi e non riconducibili alla persona i dati personali trattati attraverso sistemi informatici, ad esempio attraverso l'uso di identificativi numerici in sostituzione del nome e cognome della persona.	✓		
MPD-5	**Controllo degli accessi logici ed autenticazione**	Misure volte ad attuare e implementare la politica di controllo degli accessi logici ai dati personali trattati attraverso sistemi informatici (ad es., politiche di accesso ad applicativi o a cartelle di rete condivise), secondo ruoli e responsabilità definite e profili personali attribuiti agli utenti. Tale politica si basa sul principio della minima conoscenza: ogni utente ha accesso ai soli dati personali strettamente necessari per lo svolgimento dei propri compiti.	✓		✓
MPD-6	**Cancellazione sicura**	Misura adottata allo scopo di eliminare e distruggere irreversibilmente i dati personali, ad esempio attraverso la smagnetizzazione di un supporto informatico o la distruzione di documenti cartacei, in modo che non possano essere recuperati dal supporto su cui sono archiviati.	✓	✓	✓

Misure generali di sicurezza fisica e logica

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
MGS-1	**Sicurezza dell'ambiente operativo**	Misure adottate per gestire la configurazione di sicurezza di server e database che costituiscono la spina dorsale del sistema di elaborazione dei dati personali, applicando politiche specifiche in funzione della rilevanza dei dati personali trattati dall'applicazione ospitata. Tali misure si applicano anche alla protezione delle applicazioni, in particolare di quelle Web.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT, es file server)	
MGS-2	**Sicurezza della rete e delle comunicazioni**	Misure adottate per proteggere i dati personali durante il transito attraverso la rete, sia per le connessioni esterne (Internet), sia per l'interconnessione con i sistemi del MIUR. A seconda della tipologia di canale sul quale il trattamento è effettuato, gli strumenti di protezione adottati comprendono: firewall, sonde di rilevamento intrusione e altri dispositivi attivi o passivi di sicurezza della rete, protocolli di cifratura, politiche di controllo dei cookies, etc.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura di rete)	
MGS-3	**Tracciatura e monitoraggio**	Misure per la registrazione delle attività eseguite su sistemi informatici dagli utenti e dagli amministratori di sistema su dati personali e sistemi di sicurezza, al fine di consentire il tracciamento delle operazioni svolte. Il monitoraggio delle registrazioni prodotte (c.d. "file di log"), inoltre, consente l'identificazione di potenziali tentativi interni o esterni di violazione del sistema e la rilevazione tempestiva di incidenti relativi a dati personali (ad es., eventi di diffusione, modifica o distruzione non autorizzate di dati personali), fornendo al tempo stesso gli elementi di prova nel contesto delle indagini.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT)	
MGS-4	**Gestione sicura del cambiamento**	Esistenza ed attuazione di un processo operativo di gestione sicura del cambiamento al fine di controllare, attraverso verifiche e approvazioni, le modifiche eseguite nel sistema IT utilizzato per il trattamento dei dati personali. Ogni modifica deve essere registrata e la data/orario dell'ultima modifica deve essere conservata.	✓		

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
MGS-5	**Gestione sicura dell'hardware, delle risorse e dei dispositivi**	Misure adottate per gestire l'inventario e la configurazione di sicurezza dell'hardware, delle risorse di rete e dei dispositivi (server, periferiche, dispositivi di comunicazione, etc.) utilizzati per il trattamento dei dati personali.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT)	
MGS-6	**Gestione sicura delle postazioni di lavoro**	Misure adottate per gestire la configurazione di sicurezza delle postazioni di lavoro degli utenti fisse e portatili (ad es., impostazioni del sistema operativo, applicazioni, software di *office automation*, etc.). Tali politiche impediscono agli utenti di eseguire azioni che potrebbero compromettere la sicurezza del sistema IT (ad es., la disattivazione di programmi antivirus o l'installazione e l'esecuzione di software non autorizzato, accesso a siti potenzialmente pericolosi).	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT)	
MGS-7	**Backup e Continuità operativa**	Esistenza ed attuazione di politiche che stabiliscono le modalità di salvataggio dei dati personali, allo scopo di assicurarne la disponibilità e l'integrità nel tempo, e di ripristino dell'operatività a seguito di un evento avverso, ossia le procedure operative e le misure tecniche da seguire per ripristinare la disponibilità e l'accesso ai servizi essenziali in caso di incidente che ne pregiudichi l'operatività.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT)	
MGS-8	**Manutenzione delle apparecchiature**	Esistenza e attuazione di politiche per la manutenzione periodica delle apparecchiature di continuità elettrica, dei sistemi antincendio e di ogni altra tipologia di sistema a supporto dell'operatività dei sistemi informativi.	✓	✓	
MGS-9	**Protezione dalle fonti di rischio ambientali**	Misure adottate per ridurre o contenere i rischi connessi a minacce ambientali (fenomeni climatici, incendi, allagamenti) che potrebbero influire sull'operatività dei sistemi informativi, sulla continuità dei servizi erogati e sulla sicurezza dei dati personali trattati. Esempi sono: gruppi di continuità, sistemi antincendio, armadi ignifughi, etc.	✓	✓	✓

Misure organizzative e processi di governo

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
MOG-1	**Modello Organizzativo e di Gestione**	Il modello organizzativo e di gestione della privacy costituisce il fondamento per la sicurezza dei dati personali trattati dall'organizzazione, definendo i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le libertà delle persone interessate e individuando ruoli e responsabilità di chi ha accesso ai dati personali, in base al principio del minimo privilegio. Un ruolo di particolare importanza è svolto dal Responsabile della Protezione dei Dati (RPD), che monitora la conformità al regolamento e collabora con il Titolare nell'adeguare le misure di protezione dei dati personali trattati.	✓	✓	✓
MOG-2	**Politiche e procedure per la protezione dei dati personali**	La politica per la protezione dei dati personali dimostra l'impegno generale alla protezione dei dati personali e definisce i principi di base per la loro sicurezza e protezione. Il documento formalizza gli obiettivi e le regole da applicare nel campo della protezione dei dati e costituisce la base per l'attuazione delle misure tecniche e organizzative specifiche richieste dall'art. 32 del RGPD. Le specifiche misure tecniche e organizzative attuate sono descritte in procedure operative di dettaglio che indirizzano temi specifici (ad esempio controllo degli accessi, gestione dei dispositivi, gestione delle risorse, ecc.).	✓	✓	✓
MOG-3	**Gestione dei Responsabili del trattamento e delle terze parti**	I rapporti con fornitori esterni di servizi che hanno accesso a o trattano dati personali per conto del Titolare devono essere formalizzati tramite un contratto o altro atto legale stabilito e siglato tra le parti, in cui è disciplinato il trattamento da parte del responsabile e specificate le misure tecniche e organizzative adottate nel rispetto dei requisiti del RGPD e a garanzia della tutela dei diritti dell'interessato.	✓	✓	✓
MOG-4	**Sicurezza del ciclo di vita delle applicazioni e nei progetti**	Misure specifiche predisposte per garantire che si considerino i requisiti di protezione dei dati personali e l'applicazione delle più severe impostazioni sulla privacy sin dalle prime fasi del processo di sviluppo di un sistema informativo e durante il ciclo di vita delle applicazioni, nel rispetto dei principi di "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*" introdotti dall'art. 25 del RGPD.	✓	✓	

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
MOG-5	**Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali**	Nel caso si verifichino incidenti di sicurezza che comportano la "*distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati*" (cfr. art. 4.12 del RGPD), sono attivate procedure per la gestione di tali eventi e la notifica all'autorità di controllo e alle persone interessate.	✓	✓	✓
MOG-6	**Gestione e formazione del personale**	Misure specifiche predisposte per garantire che il personale coinvolto nel trattamento dei dati personali sia adeguatamente informato in merito agli obblighi di riservatezza, specialmente per il personale chiave coinvolto nel trattamento dei dati personali ad alto rischio, e sensibilizzato sulle procedure di sicurezza e protezione dei dati (ad esempio uso di password e accesso a specifici sistemi di elaborazione e trasmissione dati).	✓	✓	✓
MOG-7	**Controllo degli accessi fisici**	Misure volte ad assicurare la sicurezza fisica e il controllo degli accessi agli edifici e alle zone in cui sono ospitate le risorse a supporto del trattamento (documenti cartacei e strumenti informatici), ad esempio attraverso un servizio di portineria, l'uso di tornelli con autenticazione tramite badge di riconoscimento e porte chiuse a chiave.	✓	✓	✓
MOG-8	**Sicurezza dei documenti cartacei**	Politiche e processi di gestione dell'archivio per assicurare che i documenti cartacei contenenti dati personali utilizzati durante il trattamento siano prodotti, archiviati, consultati, trasmessi e distrutti nel rispetto dei diritti dell'interessato.			✓

Criteri di valutazione dei rischi

Finalità del trattamento

Il principio di finalità (o limitazione della finalità) dei dati prevede che un trattamento di dati personali è legittimo in relazione, appunto, al fine del trattamento stesso.

La finalità risponde alla domanda "perché" trattare i dati. I dati devono essere raccolti per finalità determinate, esplicite e legittime. Cioè il titolare del trattamento deve stabilire prima dell'inizio del trattamento gli scopi (che non devono essere generici o indefiniti o illimitati) in base ai quali ha intenzione di raccogliere e trattare i dati personali, deve comunicare in maniera chiara e comprensibile (principio di trasparenza) agli interessati tali finalità a mezzo dell'apposita documentazione (informativa) che deve essere portata a conoscenza dell'interessato, in modo da permettere all'interessato di fornire un consenso informato, e messa a disposizione a fini di ispezione da parte delle autorità di controllo. In assenza della precisazione della finalità, il trattamento è illegittimo.

I dati, infine, devono essere trattati secondo modalità compatibili con le finalità indicate. Stabilire gli scopi del trattamento, e esplicitarli nelle comunicazioni all'interessato, aiuta a comprendere ciò che è davvero necessario e quindi a non raccogliere dati superflui.

Mutamento di finalità

Il trattamento è strettamente legato alla finalità iniziale. Nell'ambito della normativa europea, quindi, non è possibile mutare la finalità e trattare i dati per fini diversi solo perché sono già stati acquisiti. Occorre, invece, chiedere un nuovo consenso agli interessati per la nuova finalità o stabilire una nuova base giuridica. L'attuale normativa prevede, però, la possibilità di trattare i dati per finalità differenti purché compatibili. La Convenzione 108 prevede la possibilità di trattare i dati per finalità "compatibili" con quelle iniziali, anche se poi non fornisce una interpretazione del concetto di "compatibilità".

Ad esempio, l'art. 5, par. 1, lett. b, del GDPR prevede l'ulteriore trattamento ai fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici. Tale tipo di trattamento comunque deve essere realizzato in base ad apposite garanzie, come previste dall'art. 89 del GDPR, al fine di tutelare i diritti degli interessati. Le garanzie, ovviamente, sono date dalle misure di sicurezza (tra le quali si può includere la pseudonimizzazione), e il rispetto della minimizzazione dei dati.

Il novellato Codice Privacy (art. 110-bis) stabilisce che l'Autorità di controllo può autorizzare il trattamento ulteriore dei dati per fini di ricerca scientifica o per finalità statistiche da parte di soggetti che svolgano principalmente tali attività, qualora l'informazione agli interessati risultasse impossibile o implicasse uno sforzo sproporzionato, però a condizione che vengano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi degli interessati, ivi incluse forme preventive di minimizzazione e di anonimizzazione dei dati.

Inoltre, il paragrafo 4 dell'articolo 6 del regolamento europeo (GDPR) prevede casi nei quali è possibile trattare dati per finalità differenti rispetto a quella della raccolta iniziale. Tale norma è una sostanziale novità dovuta all'ampliamento dei trattamenti, specialmente in relazione alle ipotesi di contitolarità (joint controllers).

In particolare il trattamento per finalità ulteriori può essere basato:

- sul consenso;
- su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1 (es. sicurezza nazionali, prevenzione dei reati, difesa, sicurezza pubblica, ecc...).

Al di là di tali due ipotesi, è possibile trattare dati per finalità compatibili, laddove per stabilire la compatibilità della nuova finalità occorre tenere conto, tra l'altro:

- di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
- del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
- della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
- delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
- dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Consenso al trattamento

Il consenso è una delle basi giuridiche del trattamento, nell'ambito del regolamento generale per la protezione dei dati personali.

E' importante tenere presente che il consenso è solo una delle sei basi giuridiche previste dal GDPR, ed è specifico dovere del titolare del trattamento valutare quale tra esse è la base giuridica più idonea per il trattamento che intende porre in essere.

Chiedere il consenso dovrebbe essere ritenuta una richiesta insolita, spesso indica che il titolare vuole sottoporre i dati personali dell'interessato ad un trattamento che l'interessato potrebbe non gradire oppure non essere in grado di aspettarsi ragionevolmente. Il consenso era centrale con la vecchia normativa che instaurava una relazione tra titolare ed interessato, per cui c'era una visione proprietaria del dato, e occorreva il consenso per poterlo trattare. Oggi non è più così, considerato che un cittadino è costantemente soggetto a numerosi trattamenti per cui la tutela della circolazione del dato è essenziale come la tutela dello stesso dato. Anche perché a seconda della base giuridica variano i diritti dell'interessato.

Definizione

Il consenso, in base al nuovo Regolamento Generale (art. 4 GDPR), è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei dati personali che lo riguardano. Il presupposto indefettibile è che il soggetto che conferisce il consenso abbia la capacità giuridica per farlo.

Inoltre, in base al Considerando 32: "il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".

Caratteristiche

Se il titolare decide di basare il trattamento sul consenso deve assicurarsi che esso presenti le seguenti caratteristiche:

1) inequivocabile;

2) libero;

3) specifico;

4) informato;

5) verificabile;

6) revocabile.

1) Consenso inequivocabile (unambiguous nella versione inglese) vuol dire che non è necessario che sia esplicito ma può anche essere implicito (ma non tacito), purché, nel momento in cui sia desunto dalle circostanze, non sussista alcun dubbio che col proprio comportamento l'interessato abbia voluto comunicare il proprio consenso (es. l'inerzia non può costituire manifestazione di consenso, come anche i form precompilati e caselle già prespuntate). Cioè deve prevedere una chiara azione positiva (come spuntare una casella od inserire la mail in un campo dove è specificata la finalità per la quale sarà usato il dato).

Il Considerando 32 del GDPR recita: “il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l’interessato manifesta l’intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un’apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell’informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l’interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l’inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell’interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso”.

Il consenso deve, invece, essere esplicito (art. 9 GDPR) nel caso di trattamento di dati sensibili o nel caso di processi decisionali automatizzati (es. profilazione).

Occorre dire che la versione originaria della proposta della Commissione europea prevedeva sempre il consenso esplicito, poi si è pervenuti al compromesso attuale.

Il consenso esplicito si può avere con una dichiarazione scritta e firmata dall'interessato o tramite l'invio di un'email indicante che la persona accetta espressamente il trattamento di determinate categorie di dati, oppure raccogliendo il consenso in due passaggi: inviare un'email all'interessato, che poi dovrò confermare la prima azione di consenso.

2) Il consenso deve essere dato liberamente, il ché significa che l'interessato deve essere in grado di operare una scelta effettiva, senza subire intimidazioni o raggiri, né deve subire conseguenze negative a seguito del mancato conferimento del consenso. L’articolo 7 del GDPR chiarisce che “nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto”.

Ad esempio, nel caso di pubblicità commerciale, il consenso deve essere separato rispetto al consenso per la prestazione contrattuale richiesta dall'utente, perchè l'utente deve avere la possibilità di addivenire al contratto senza dover subire il ricatto di dover ricevere pubblicità commerciale. Non può definirsi libero il consenso a ulteriori trattamenti dei dati personali che l'interessato debba prestare quale condizione per conseguire una prestazione richiesta (provvedimento del Garante del 31 gennaio 2008).

Questo purtroppo porta al rischio che molti dei consensi ottenuti dai servizi online possano essere ritenuti invalidi. Lo stesso Gruppo Articolo 29 fornisce un esempio chiarificatore: una app mobile per il fotoritocco chiede il consenso per accedere alla geolocalizzazione e i dati vengono utilizzati a fini di pubblicità comportamentale. Ma né la geolocalizzazione, né la pubblicità sono necessari per la fornitura del servizio (fotoritocco), per cui subordinare l'uso della App a tale consenso rende il consenso non libero e quindi illecito.

Sul punto la Corte di Cassazione italiana, con la sentenza n. 17278/2018, ha precisato che il gestore di un sito concernente un servizio fungibile e rinunciabile può negare l'accesso al servizio all'utente che non acconsenta al trattamenti dei propri dati per finalità commerciali. In questo caso il punto focale sta nella fungibilità e rinunciabilità del servizio. Il blocco dell'accesso al sito non pottrebbe essere imposto nel caso in cui il sito offra un servizio essenziale per l'utente. La Corte sostiene che ciò che è interdetto al gestore di "utilizzare i dati personali per somministrare o far somministrare informazioni pubblicitarie a colui che non abbia la volontà di riceverli".

Il Garante ha, però, ribadito, successivamente, col provvedimento del 12 giugno 2019, che la libertà del consenso "non è assicurata né quando viene richiesto un unico consenso per più diverse finalità di trattamento, né quando si assoggetta la fruizione di un servizio […] alla previa autorizzazione a trattare i dati conferiti, ai fini di tale servizio, per finalità diverse qual è quella di promozione e quella statistica". In tal senso appare un evidente contrasto tra Suprema Corte e Garante.

Un altro problema riguarda il consenso dei dipendenti. Se il datore di lavoro richiede il consenso all'utilizzo del dato (es. vuole pubblicare la foto dei dipendenti sul sito web aziendale) e vi è un pregiudizio reale o potenziale per il cliente non consenziente (cosa altamente probabile in un contesto lavorativo), il consenso non può ritenersi valido perché non libero. Dato lo squilibrio di potere tra datore e dipendente, quest'ultimo può dare un consenso valido solo in circostanze eccezionali. Quindi, il consenso non può costituire la base giuridica del trattamento in caso di evidente squilibrio tra le parti. In tal caso sarebbe preferibile trattare i dati su base giuridica differente.

3) Il consenso deve essere specifico, cioè relativo alla finalità per la quale è eseguito quel trattamento (granularità del consenso). Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per ogni finalità (Considerando 32 GDPR). Quindi, i dati dovranno essere pertinenti al consenso fornito, e in caso di modifiche del trattamento occorre richiedere un nuovo consenso. Per cui avremo un consenso per il marketing diretto, un consenso per la profilazione, ecc...

Nel caso di titolari congiunti ogni titolare deve acquisirte il consenso relativamente alle proprie finalità. Ad esempio, il gestore di un sito web che utilizza plugin di Facebook dovrà chiedere il consenso con riferimento alla sola raccolta dei dati e successiva comunicazione a Facebook.

Un caso classico riguarda i cookie. Il consenso deve essere specifico in relazione alla finalità dei cookie, non può essere unico per tutti i cookie se questi hanno finalità differenti.

4) Il consenso deve essere informato, occorre cioè che l'interessato sia posto in condizioni di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge, cioè deve essere rispettato il principio di trasparenza. Inoltre l'interessato deve essere opportunamente informato sulle conseguenze del suo consenso (ad esempio deve essere indicato che in assenza di consenso non potrà accedere a determinate sezioni del sito web). L'informazione si ha attraverso l'apposita informativa, che in questo caso diventa una vera e propria condizione di legittimità del trattamento. Il regolamento europeo si concreta, più che sui requisiti formali del consenso, sulla necessità della validità sostanziale del consenso, per cui l'aspetto informativo è essenziale, richiedendo un linguaggio semplice e comprensibile, anche eventualmente colloquiale.

5) Consenso verificabile non vuol dire che il consenso deve essere documentato per iscritto, né che è richiesta la forma scritta (anche se in alcune ipotesi -es. dati sensibili- può essere preferibile perché consente più facilmente di provare il consenso, facilitando quindi le verifiche da parte dell'autorità),

ma che l'azienda deve essere in grado di dimostrare che l'interessato lo ha conferito con riferimento a quello specifico trattamento (quindi distinguendo tra i vari trattamenti). L'azienda dovrà essere in grado di sapere anche a quale informativa l'utente ha acconsentito, distinguendo tra le varie versioni.

Il WP29 suggerisce di utilizzare un registro nel quale siano conservate le informazioni relative alla sessione in cui è stato espresso il consenso, unitamente alla documentazione del flusso di lavoro del consenso, e una copia delle informazioni presentate all'interessato in quel momento.

6) Il consenso deve essere revocabile in qualsiasi momento. La revoca deve essere facile così come lo è dare il consenso. Non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi (ovviamente la revoca non comporta illiceità del trattamento precedente, ma solo l'obbligo di terminare il trattamento), a meno che non sussista una differente base giuridica per continuare il trattamento.

Per revocare il consenso, quindi, il titolare dovrebbe predisporre una procedura analoga a quella offerta per concedere il consenso. In alternativa è possibile revocare il consenso inviando una comunicazione, o tramite un apposito form sul sito, o tramite mail, ai contatti indicati nel sito all'interno dell'informativa (interpello al titolare). Nel caso in cui il titolare non ottemperi, ci si può rivolgere al Garante o al tribunale per la tutela dei propri diritti.

Con la revoca si innesca il diritto di cancellazione, per cui l'azienda deve cancellare i dati dell'utente. Ovviamente vi sono motivi legittimi in base ai quali un'azienda ha necessità di conservare alcuni dati dell'utente anche dopo la revoca del consenso, come ad esempio mantenere un registro delle transazioni per motivi fiscali. In ogni caso l'azienda può avvertire l'interessato che a seguito della revoca del consenso, vi sarà la cancellazione dei dati è la conseguente impossibilità di fornire ulteriori servizi.

Scadenza

Occorre tenere presente che il consenso non dura per sempre. Quando si raccolgono dati personali occorre informare l'interessato della durata della conservazione (e quindi trattamento) del dato, scaduta la quale il dato va o anonimizzato oppure cancellato. Per questo motivo in alcuni casi potrebbe essere preferibile una base giuridica diversa dal consenso, come ad esempio i legittimi interessi del titolare del trattamento.

Dati soggetti a trattamento speciale

Per i dati soggetti a trattamento speciale, cioé quelli che una volta si definivano dati sensibili, con in più i dati biometrici e genetici, sussiste un generale divieto di trattamento, con una serie di esenzioni, tra i quali il consenso esplicito. A parte, ovviamente, il trattamento per l'attività giornalistica, che è a forma libera per qualsiasi tipo di dato.

Minori

Il consenso dei minori è valido a partire dai 16 anni di età. Prima dei 16 anni occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Portabilità dei dati

Se il trattamento dei dati è basato sul consenso dell'interessato, questi acquisisce l'ulteriore diritto alla portabilità dei dati.

Consenso e regolamento Privacy

Il consenso è un prerequisito del regolamento Privacy. Quest'ultimo, infatti, nel disciplinare le comunicazioni elettroniche, compreso i cookie, fa riferimento alla definizione di consenso contenuta nella normativa generale, che oggi è il regolamento europeo. Di conseguenza nell'applicare la Privacy occorre sempre fare riferimento al consenso di cui al GDPR. Ad esempio, nella gestione dei cookie occorre che il consenso sia specifico, cioé separato per finalità.

Interessato al trattamento

L'interessato (data subject) al trattamento è la persona fisica a cui si riferiscono i dati personali.

Il concetto di interessato è cambiato rispetto al passato, nel senso che oggi siamo tutti potenzialmente interessati in considerazione del fatto che i trattamenti dei dati personali inglobano l'intera società. Basti pensare alle telecamere di controllo del traffico, le fidelity card, e cosi via, per comprendere che in ogni istante siamo potenziali interessati di un trattamento. Il concetto di interessato, quindi, è dinamico.

L'interessato, inoltre, può essere solo una persona fisica, e non una persona giuridica, un ente o un'associazione, come chiarito dal Considerando 14 del GDPR. Anche se ciò non necessariamente significa che una persona giuridica non possa subire dei danni a seguito di un trattamento di dati. Nel qual caso potrà intentare azione di risarcimento del danno ai sensi delle norme del codice civile (art. 2043 c.c.) senza però potersi avvaleri dei vantaggi della disciplina di cui al GDPR (art. 2050 c.c.).

Diritti dell'interessato

La normativa attribuisce specifici diritti all'interessato, il quale, per l'esercizio di tali diritti, può rivolgersi direttamente al titolare del trattamento. L'interessato può esercitare i suoi diritti anche in un momento successivo a quello in cui ha prestato il consenso, potendo così revocare un consenso già prestato.

I diritti esercitabili dall'interessato sono i seguenti:

- diritto di ottenere informazioni su quali dati sono trattati dal titolare (diritto di informazione);

- diritto di chiedere ed ottenere in forma intellegibile i dati in possesso del titolare (diritto di accesso);

- diritto di revocare il consenso in qualsiasi momento;

- esercitare l'opposizione al trattamento in tutto o in parte;

- diritto di opporsi ai trattamenti automatizzati e a non essere assoggettati a trattamenti basati esclusivamente su decisioni automatizzate compreso la profilazione.

- diritto di ottenere la cancellazione dei dati in possesso del titolare;

- diritto di ottenere l'aggiornamento o la rettifica dei dati conferiti;

- diritto di chiedere ed ottenere trasformazione in forma anonima dei dati;

- diritto di chiedere ed ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento;

- diritto alla portabilità dei dati.

Diritto di informazione

In base al principio di correttezza e trasparenza, l'interessato al trattamento ha il diritto di ricevere una corretta e completa informazione in relazione a:

- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

- categorie di dati personali trattate;

- destinatari dei dati o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali, e le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi;

- finalità e base giuridica del trattamento;

- eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione, nel qual caso il titolare deve informare l'interessato, esplicitando le modalità e le finalità della profilazione, nonché

la la logica inerente il trattamento e le conseguenze previste per l'interessato a seguito di tale tipo di trattamento;

- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

- i diritti previsti dal Regolamento e le modalità per esercitarli, in particolare l'esistenza del diritto di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che riguardano l'interessato o di opporsi al loro trattamento, e l'esistenza del diritto di proporre reclamo a un'autorità di controllo;

- qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate rispetto alla tutela fornita nel paese terzo.

Tutto ciò avviene a mezzo dell'informativa, il cui scopo è, appunto, informare l'interessato.

Diritto di accesso

L'art. 15 del regolamento europeo prevede il diritto di accesso, cioè il diritto di conoscere quali dati personali relativi all'interessato il titolare sta trattando, con quali finalità (non le modalità invece), e di ricevere eventualmente una copia (gratuita, a parte il costo del supporto) dei dati. I titolari possono eventualmente anche consentire un accesso diretto ai dati da remoto.

Diritto di opposizione

In base all'art. 21 del regolamento europeo, l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano connessi a ragioni di interesse pubblico o all'esercizio di pubblici poteri (ai sensi dell'articolo 6, paragrafo 1, lettera e). Si tratta di un diritto che trova la sua ragione di essere nella tutela dell'individuo dal controllo eccessivo dello Stato.

L'interessato può opporsi anche al trattamento posto in essere per il perseguimento di legittimi interessi del titolare o di terzi (art. 6, par. 1, lett. f), compresa la profilazione sulla base di tali disposizioni.

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

L'interessato può opporsi anche al trattamento dei dati per fini commerciali, come marketing diretto e profilazione. L'opposizione al trattamento è operazione diversa dalla cancellazione dei dati. In base ad essa l'interessato può impedire il trattamento che non è compatibile con le finalità del consenso. Nel

caso di trattamenti basati sul consenso, comunque, prevale la possibilità di revoca del consenso rispetto al diritto di opposizione.

Diritto di aggiornamento e rettifica

L'interessato (art. 16 GDPR) può rivolgersi al titolare del trattamento per ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, ha anche il diritto di ottenere l'integrazione dei dati incompleti, eventualmente fornendo una dichiarazione integrativa. E' uno dei diritti che consente all'interessato di mantenere un controllo attivo sui propri dati, potendone ottenere la correzione, la modifica, l'aggiornamento e l'integrazione, così evitando che il loro uso, compreso il trasferimento, possa generare dei pregiudizi per l'interessato.

Diritto di limitazione del trattamento

Il diritto di limitazione (art. 18 del regolamento) consente all'interessato di ottenere il blocco del trattamento nelle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza;

- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

- benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

- l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

In caso di esercizio di tale diritto ogni trattamento, tranne la conservazione, è vietato. Il dato deve essere contrassegnato in attesa delle ulteriori valutazioni da parte del titolare. Il Considerando 67 precisa che "negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato".

Diritto alla cancellazione (oblio)

Il diritto alla cancellazione (anche detto diritto "all'oblio") è un nuovo diritto che consente di ottenere la cancellazione dei propri dati personali in casi particolari. Può essere esercitato anche dopo la revoca del consenso.

Diritto alla portabilità

Il diritto alla portabilità dei dati è un nuovo diritto previsto dal regolamento europeo. Si applica solo ai trattamenti automatizzati basati sul consenso o sulla necessità contrattuale, e sono previste specifiche condizioni per il suo esercizio.

Esercizio dei diritti

L'interessato può rivolgersi direttamente al titolare del trattamento per l'esercizio dei suoi diritti (interpello). Anche se è solo il titolare obbligato a dare riscontro, il responsabile del trattamento è tenuto a collaborare col titolare ai fini dell'esercizio dei diritti.

E' il titolare del trattamento che deve dare riscontro alla richiesta dell'interessato, entro un mese dall'esercizio del diritto. Il termine di un mese può essere esteso a 3 mesi in casi di particolare complessità. In questo caso il titolare del trattamento deve comunque avvertire l'interessato entro il mese. L'unico obbligo per l'interessato è di fornire i dati per la sua identificazione.

L'esercizio dei diritti è in linea di massima gratuito. Spetta comunque al titolare valutare se la risposta è complessa al punto da dover chiedere un contributo all'interessato, e stabilirne l'ammontare, ma solo se si tratta di richieste manifestamente infondate o eccessive o ripetitive (sul punto il Garante italiano dovrebbe pubblicare delle linee guida, per il momento si può fare riferimento alla delibera del 2004 Contributo spese in caso di esercizio dei diritti dell'interessato).

La risposta si deve fornire di regola in forma scritta, anche attraverso strumenti elettronici. Può essere orale solo se espressamente richiesta in tal senso dall'interessato. La risposta deve essere chiara, coincisa, e facilmente accessibile e comprensibile.

In caso di mancata risposta, o di risposta inadeguata, può rivolgersi all'autorità amministrativa (Garante) o giudiziaria per la tutela dei suoi diritti.

Deroghe all'esercizio dei diritti

L'articolo 23 del GDPR consente agli Stati membri di limitare i diritti degli interessati, per diversi motivi tra cui la sicurezza nazionale e pubblica, per motivi di interesse generale e così via. Tali restrizioni devono rispettare l'essenza dei diritti e delle libertà fondamentali e devono essere a misura necessaria e proporzionata in una società democratica.

Tali limitazioni devono essere previste dalle disposizioni nazionali. In tale prospettiva si ritiene possano essere ancora applicate le deroghe stabilire dall'articolo 8 del Codice per la protezione dei dati personali italiano, e cioè nei casi in cui il trattamento dati è effettuato:

a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;

b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;

c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;

e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;

f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;

g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;

h) ai sensi dell'articolo 53 (trattamenti da parte di forze di polizia), fermo restando quanto previsto dalla legge 1 aprile 1981, n. 121.

Misure di sicurezza

Il regolamento europeo dedica alla problematica delle misure di sicurezza vari articoli, anche in considerazione dell'accresciuta sensibilità alla pericolosità delle varie forme di trattamento dei dati personali.

Principio di sicurezza

L'art. 5, par. 1, lett. f), stabilisce che i dati personali devono essere "trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal

danno accidentali («integrità e riservatezza»)". E' importante notare che è l'intero trattamento a dover essere sicuro, non solo i dati come prodotto finale. Ciò comporta anche che le valutazioni di sicurezza vanno sviluppate per ogni tipo di trattamento.

L'art. 32, invece, fissa alcuni principi fondamentali. In particolare le misure di sicurezza devono essere approntate "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche".

Le misure di sicurezza, quindi, devono essere adeguate, imponendo non un'obbligazione di risultato, bensì un'obbligazione di mezzi, in modo che le misure siano ragionevolmente soddisfacenti alla luce delle conoscenze e delle prassi.

Le misure di sicurezza si dividono in due categorie: misure organizzative e misure tecniche, che, sempre secondo l'art. 32, comprendono, tra le altre:

misura tecnica -> a) la pseudonimizzazione e la cifratura dei dati personali;

requisiti di sicurezza -> b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La sicurezza, infatti, non riguarda solo l'aspetto informatico del trattamento, ma anche l'aspetto organizzativo a coprire eventi quali la sottrazione o la perdita di documenti. Le misure di sicurezza, quindi devono garantire che:

- i dati possono essere consultati, modificati, divulgati o cancellati solo dalle persone autorizzate a farlo (e che tali persone agiscono solo nell'ambito dell'autorità che gli viene concessa);

- i dati trattati sono accurati e completi in relazione al motivo per cui lo stai elaborando;

- i dati rimangono accessibili e utilizzabili, cioè, in caso di perdita, modifica o distruzione accidentale, si deve essere in grado di recuperarli e prevenire danni alle persone interessate, predisponendo un opportuno piano di continuità operativa.

Il principio di sicurezza, quindi, prevede l'obbligo di riservatezza, integrità e disponibilità dei dati.

Analisi del rischio

Il regolamento europeo ha un approccio basato sulla valutazione del rischio piuttosto che sulla protezione dell'utente. Per cui occorre una corretta analisi dei rischi del trattamento dei dati personali per poter implementare le misure di sicurezza adeguate.

Lo stesso art. 32, par. 2, elenca alcuni tipi di rischio:

- distruzione o perdita di dati;

- modifica;

- divulgazione non autorizzata;

- accesso, in modo accidentale o illegale, non autorizzato.

Per ogni rischio occorre individuare la probabilità dell'evento, nonché la gravità dello stesso, in modo da stabilire le misure di sicurezza adeguate per mitigare il rischio. Un esempio classico riguarda la dismissione delle stampanti con memoria, senza aver provveduto a cancellare la memoria, e quindi con l'astratta possibilità che un terzo possa acquisire le immagini ottiche degli ultimi documenti stampati o scansionati.

Codici di condotta e certificazioni

Sempre in base all'art. 32, "l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo".

Cioè gli organismi rappresentanti di categorie o le associazioni di aziende possono elaborare dei codici di condotta che aiutino i titolari ad applicare correttamente il regolamento europeo. In tal modo, quindi, gli oneri per le imprese vengono semplificati. Il titolare, infatti, con risparmio di spesa, si limiterà ad adottare il codice di condotta senza dover elaborare le misure organizzative e di sicurezza. I codici di condotta sono, quindi, delle misure di garanzia, che vengono sottoposti all'approvazione delle autorità di controllo nazionali, incaricate di vigilare sull'attuazione dei medesimi codici. Ovviamente il titolare, e il responsabile se nominato, dovranno tenersi sempre aggiornati sulla disponibilità e l'evoluzione dei codici di condotta.

Analogamente, l'adozione di processi di trattamento certificati può essere utilizzato a dimostrazione del concreto impegno da parte del titolare nell'attuazione del regolamento.

Sia i codici di condotta che le certificazioni non esimono i titolari da responsabilità, ma sicuramente possono essere degli elementi di valutazione nel momento in cui si debba stabilire la quantità di responsabilità e quindi il risarcimento del danno (art. 83 lett. J GDPR).

Misure di sicurezza fisiche

Per approntare delle misure di sicurezza è necessario valutare fattori quali:

- la qualità delle porte e delle serrature e la protezione dei locali con allarmi, illuminazione di sicurezza o CCTV (telecamere);

- l'accesso ai tuoi locali e il controllo dei visitatori;

- il corretto smaltimento dei rifiuti cartacei o elettronici;

- la sicurezza delle apparecchiature informatiche, in particolare i dispositivi mobili (è utile tenere un registro con l'indicazione delle risorse informatiche utilizzate per trattare dati, la loro ubicazione fisica e i permessi di accesso alle stesse).

Misure di sicurezza informatiche (o logiche)

Fattori da considerare per la sicurezza informatica:

- sicurezza della rete e dei sistemi di informazione (sistemi di autenticazione);

- sicurezza dei dati conservati nel sistema (controlli di accesso);

- sicurezza online (sito web o applicazioni online);

- sicurezza dei dispositivi, in particolare quelli personali se usati per motivi aziendali.

I sistemi di autenticazione devono essere configurati in modo da controllare gli accessi ai dispositivi e agli applicativi, tramite credenziali (username e password). La politica in materia di password dovrebbe essere definita a documentata, con indicazione della lunghezza minima e dei criteri per la scelta delle password. Ancora meglio sarebbe utilizzare sistemi di verifica a due fattori (2FA)

Sarebbe preferibile avere profili con privilegi distinti e compiti separati.

Diritto alla cancellazione

Il diritto alla cancellazione (impropriamente detto diritto all'oblio) nasce come evoluzione del principio sancito dalla sentenza della Corte di Giustizia europea del 13 maggio 2014.

Con detta sentenza la Corte del Lussemburgo ha stabilito il diritto di una persona ad ottenere la deindicizzazione di un link relativo a una notizia che la riguarda quando tale notizia non ha più interesse pubblico. Ovviamente il diritto alla cancellazione riguarda i dati personali, e non solo le notizie. Si tratta dell'ovvia estensione del concetto che i dati possono essere trattati solo per il tempo necessario per soddisfare lo scopo del trattamento. Il diritto riguarda sia i dati trattati elettronicamente che quelli cartacei. Occorre, quindi, predisporre apposite procedure per ottemperare alle richieste.

Il diritto alla cancellazione non è un diritto assoluto bensì un limite esterno al diritto di cronaca e alla libertà di stampa, in tal senso va opportunamente bilanciato col diritto in competizione. Ciò vuol dire

che non sempre la richiesta sarà accolta, e comunque non necessariamente la misura a protezione deve essere la cancellazione totale delle informazioni online, ma potrebbe essere anche una misura di portata minore, purchè in grado di riequilibrare i diritti in contrapposizione, riducendo l'invasività del trattamento, come appunto può essere la mera deindicizzazione da parte del motore di ricerca (che non è una vera e propria cancellazione delle informazioni).

Requisiti

Oggi il diritto alla cancellazione (right to be forgotten) è previsto dall'articolo 17 del regolamento europeo in materia di protezione dei dati personali. L'interessato può chiedere la cancellazione dei propri dati anche dopo la revoca del consenso al trattamento. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo (da considerare quindi in pochi giorni) nei seguenti casi:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento, se non esiste alcun altro motivo legittimo per il trattamento;

c) l'interessato si oppone al trattamento e non sussiste alcun ulteriore motivo legittimo per procedere il trattamento;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori.

Il titolare del trattamento nei casi indicati è obbligato a procedere alla cancellazione dei dati e ad adottare le misure ragionevoli per informare altri titolari del trattamento che stanno trattando i dati (compreso "qualsiasi link, copia o riproduzione") di procedere alla loro cancellazione.

Tuttavia i titolari possono continuare ad elaborare i dati se sono comunque necessari per gli scopi per i quali sono stati raccolti e il titolare ha ancora una base giuridica per il trattamento degli stessi. Quindi nei casi in cui il trattamento è necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui la cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Chiedere il diritto all'oblio a Google

In sintesi, quindi, è esclusa la possibilità di ottenere il diritto all'oblio se esiste un motivo legittimo per continuare a mantenere i dati online, e in genere l'interesse pubblico alla notizia è il motivo prevalente per respingere la richiesta. Questo purché la notizia sia attuale e veritiera. Ad esempio non è ammissibile la cancellazione della notizia di un arresto se il relativo procedimento è ancora in corso. Inoltre, si può chiedere l'oblio solo con riferimento ad una ricerca effettuata utilizzando il nome e cognome come chiavi di ricerca. Per chiedere la deindicizzazione di dati dal motore di ricerca di Google ci si deve recare sull'apposita pagina predisposta dal motore di ricerca a compilare i campi. Occorre tenere presente che solo i link indicati saranno soggetti alla valutazione di Google, che non è tenuto a cercare altre pagine sulle quali è presente lo stesso dato. Soprattutto è importante indicare il contesto del fatto, perchè Google possa valutare correttamente se esiste o meno ancora un interesse pubblico alla notizia. Ad esempio, se si tratta di una condanna per reati commessi quando si era un politico e oggi non lo si è più, occorre precisare tale circostanza che risulta fondamentale per un corretto bilanciamento. Google, se accoglie la richiesta, si limita alla deindicizzazione della pagina dal motore di ricerca con riferimento al nome e cognome del richiedente, quindi la notizia in sé rimane sul sito fonte (blog, giornale, ecc...) e comunque si può rintracciarla se la ricerca viene fatta con dati dell'evento differenti dal nome e cognome del richiedente. E' possibile anche rivolgersi direttamente al sito fonte della notizia, blog, giornale, ecc..., ad esempio inviando una mail o comunque contattando il gestore del sito tramite gli strumenti indicati sul sito stesso. Il gestore non è necessariamente obbligato a cancellare la notizia, comunque dovrà valutare se sussiste ancora un interesse pubblico alla stessa. In molti casi il gestore del sito potrà procedere, in alternativa, alla rettifica della notizia o all'aggiornamento. Ad esempio, in caso di arresto, se poi è seguito un proscioglimento, il gestore potrà inserire questo nuovo dato a completare la notizia. In caso di mancato accoglimento della richiesta, da parte di Google o da parte del titolare del sito fonte, oppure anche in alternativa, ci si può rivolgere al Garante Privacy oppure ad un tribunale, per la tutela dei propri diritti.

Profilazione e processi decisionali automatizzati

Per profilazione si intende l'insieme delle attività di raccolta ed elaborazione dei dati inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento (segmentazione).

In ambito commerciale, la profilazione dell'utente è il mezzo che consente la fornitura di servizi personalizzati oppure l'invio di pubblicità comportamentale.

L'articolo 4 del nuovo Regolamento europeo definisce la profilazione come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

Il Considerando 24 specifica ulteriormente che, per stabilire se si è in presenza di profilazione "è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali".

Ovviamente la profilazione deve essere svolta utilizzando i soli dati strettamente necessari per la finalità indicata, in ossequio al principio di pertinenza e di proporzionalità.

In sintesi, si ha profilazione in presenza di 3 elementi:

- un trattamento automatizzato;

- eseguito su dati personali;

- con lo scopo di valutare aspetti personali di una persona fisica.

Ovviamente non deve trattarsi di mero "tracciamento" dell'interessato che naviga online, ma di analisi per prendere decisioni che riguardano il soggetto oppure per analizzarne o prevederne le preferenze o i comportamenti. Cioé, si è in presenza di profilazione in relazione allo scopo dei dati raccolti. Ad esempio, l'applicazione di sanzioni per eccesso di velocità, erogate sulla base delle immagini raccolte dagli autovelox non comporta alcuna valutazione di aspetti personali, per cui non costituisce profilazione.

Base giuridica

Il regolamento europeo sancisce un generale divieto di sottoporre un individuo a processi decisionali automatizzati compresa la profilazione. Ma l'articolo 22 del GDPR, paragrafo 1, chiarisce l'ambito di applicazione delle norme in materia, che è limitato alle sole ipotesi in cui l'attività il processo decisionale automatizzato:

- produce effetti giuridici

- oppure incide in modo significativo sulla persona dell'utente,

- e la decisione è basata interamente (solely) sul trattamento automatizzato dei dati.

Gli effetti legali del processo decisionale automatizzato potrebbero essere: il diniego di attraversamento di una frontiera; l'adozione di misure di sicurezza; il diniego di forme di assistenza sociale; il rifiuto di un impiego; il rifiuto della concessione di un prestito.

Esistono delle eccezioni al divieto, per cui un interessato può essere sottoposto ad un processo decisionale automatizzato, compreso la profilazione, quando:

1) il trattamento è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare (la necessità deve essere interpretata in modo restrittivo, anche se i Garanti europei precisano che motivi di efficienza -cioè in questo modo si ottengono risultati più veloci, più efficaci, quindi anche a favore dell'individuo- sono ritenuti sufficienti per giustificare l'utilizzo di sistemi decisionali basati su profilazione, a condizione che non vi siano metodi meno intrusivi che raggiungano lo stesso risultato), ma tale eccezione non si applica in caso di trattamento di dati sanitari (quindi le compagnia assicurative dovranno fare conto sulle eccezioni di cui al n. 3);

2) il trattamento è autorizzato da una legge o regolamento, che prevede altresì misure idonee a tutelare i diritti dei soggetti interessati;

3) vi è esplicito consenso al trattamento (ricordiamo che il consenso alla profilazione deve essere distinto rispetto al consenso relativo ad altri trattamenti).

Nel primo e nel terzo caso, il titolare del trattamento deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato,

Secondo il WP29 (Linee guida in materia di processi automatizzati e profilazione, 2018) la profilazione può essere basata anche sui legittimi interessi del titolare del trattamento, alla stregua del marketing diretto. Tuttavia occorre sempre effettuare il bilanciamento degli interessi per valutare l'eventuale prevalenza di quelli del titolare. Le linee guida indicano alcuni elementi da valutare:

- il livello di dettaglio del profilo;

- la completezza del profilo (se il profilo descrive solo un piccolo aspetto della persona interessata, o fa un quadro più completo);

- l'impatto della profilazione (gli effetti sull'interessato); e

- le misure di sicurezza volte ad assicurare equità, non discriminazione e accuratezza nel processo di profilazione.

Se l'acquisizione dei dati avviene attraverso l'utilizzo di cookie, si applica la relativa normativa.

Diritto di opposizione e revisione

L'interessato ha il diritto di non essere oggetto di una decisione basata esclusivamente su un trattamento automatizzato, tra cui profilazione, che produce effetti giuridici che lo riguardano. In questi casi l'interessato può opporsi a tale elaborazione. In tal caso il titolare deve immediatamente interrompere il trattamento finché non dimostra all'interessato che il trattamento automatizzato e la profilazione non violano i suoi diritti e le sue libertà.

Inoltre, l'interessato può espressamente chiedere che ogni decisione automatizzata che lo riguardi sia condizionata da un intervento umano, di poter esprimere il proprio punto di vista e contestare la decisione, con adeguate motivazioni. In breve l'interessato ha il diritto di ricevere una giustificazione della decisione automatizzata. Il WP29 sottolinea che la supervisione umana della conclusione

raggiunta dalla macchina deve essere significativa, altrimenti sarebbe solo un modo per aggirare il divieto.

Il problema sta, però, nel fatto che i sistemi automatizzati oggi sono non solo sistemi estremamente complessi, ma i loro codici sono anche soggetti ad elevati livelli di segretezza, per cui appare piuttosto difficile che il titolare (il quale spesso non è altro che l'acquirente di uno strumento di analisi automatizzata) possa fornire una giustificazione adeguata alla decisione fornita dal sistema.

Diritto all'informazione

Il titolare del trattamento deve essere trasparente, cioè deve informare gli interessati dell'esistenza di una decisione basata sul trattamento di dati automatizzato comprendente profilazione (art. 22 GDPR e Considerando 71). Nell'informativa devono, quindi, essere esplicitate le modalità e le finalità della profilazione. Inoltre, deve essere chiarita la logica inerente il trattamento e le conseguenze previste per l'interessato a seguito di tale tipo di trattamento, intendendo in tal senso i criteri utilizzati per giungere alla decisione (senza necessariamente dover fornire una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo). Ovviamente questo può essere un problema nel momento in cui l'utilizzatore del processo decisionale non ha contezza di come funzioni davvero, avendolo acquistato da terzi. Spesso, infatti, il sistema è una black box.

Un'interpretazione contestuale del GDPR mostra che effettivamente il regolamento impone ai titolari del trattamento di dimostrare la conformità agli obblighi previsti, in particolare ai requisiti di liceità, correttezza e trasparenza. Per cui, fornire informazioni sul processo decisionale automatizzato e la logica soggiacente è solo una parte del problema. Il GDPR prevede che i titolari dimostrino che le correlazioni applicate nell'algoritmo siano imparziali, cioè non discriminatorie e ci sia una legittima giustificazione alla decisione automatizzata. Gli individui soggetti alla decisione automatizzata, infatti, hanno una pluralità di diritti, quali l'opposizione alla profilazione (articolo 21), la richiesta di cancellazione o la rettifica del loro profilo (articolo 17), la contestazione alle decisioni automatizzate (articolo 22, paragrafo 3).

Tale diritto, inoltre, va evidentemente inquadrato tra i diritti degli interessati, per cui la "spiegazione" deve essere rapportata all'interessato, deve essere significativa per lui, in modo da consentirgli di esercitare gli altri suoi diritti. E quindi la spiegazione deve essere tale da porlo in condizioni da comprendere se ha subito una discriminazione.

Dati individuali o dati aggregati

La profilazione può avvenire utilizzando dati individuali o identificativi (es. dati anagrafici), oppure dati aggregati derivanti da dati personali individuali. Il livello di aggregazione è variabile, e quindi potrebbe accadere che i dati utilizzati, anche se in forma aggregata, consentano comunque, a seguito dell'incrocio con altri dati, l'identificazione dei soggetti interessati. Ecco perchè col GDPR si impone la valutazione di impatto del trattamento.

Dati sensibili

Il GDPR vieta l'utilizzo di dati personali sensibili per scopi decisionali automatizzati, a meno che:

- l'interessato non abbia espresso il suo consenso esplicito;

- o la decisione automatizzata è necessaria per motivi di interesse pubblico.

Misure di sicurezza e valutazione di impatto

Il titolare del trattamento, inoltre, deve ottemperare agli obblighi in materia di misure di sicurezza, analisi dei rischi del trattamento, formazione del personale, nomina degli amministratori di sistema, procedure di disaster recovery.

In particolare dovrà verificare se esiste un rischio di discriminazione, furto di identità, danni alla reputazione o altri effetti negativi per gli interessati.

Ad esempio, il titolare potrà adottare misure di pseudonimizzazione o minimizzazione dei dati per evitare che il trattamento automatizzato incida in misura significativa sugli interessati.

Inoltre, è opportuno che il titolare ponga in essere misure tecniche ed organizzative adeguate al fine di garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori di misure matematiche o statistiche, e che impedisca effetti discriminatori nei confronti delle persone sulla base del trattamento dei dati per attività di profilazione.

Infine, il trattamento basato su sistemi automatizzati (anche se non esclusivamente basato sulla valutazione della macchina, ma anche quello con intervento umano) deve essere preceduto dalla valutazione di impatto, proprio perché dalle elaborazioni possono derivare dettagli informativi ritenuti di natura particolarmente invasiva ma anche perché possono essere impiegati una quantità significativa di dati ai quali devono essere assicurati gli opportuni livelli di protezione e garanzia contro i possibili rischi per i diritti e le libertà degli Interessati.

Il regolamento impone altresì che il titolare adotti una politica di periodica revisione degli applicativi di decisione automatizzata, per al fine di verificare se il sistema produce errori, classificazioni non corrette e possibili discriminazioni.

L'art. 22, par. 2 prevede che lo Stato membro possa stabilire "misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato" in caso di processi decisionali automatizzati. L'Italia non ha ritenuto di prevedere ulteriori misure.

Problematiche

L'attività di profilazione è considerata estremamente invasiva e può portare a danni ed abusi a carico degli utenti. La profilazione, infatti, viene utilizzata per fornire pubblicità personalizzata agli utenti, ma può anche portare a differenti offerte commerciali (price discrimination) a seconda della persona o

della categoria nella quale essa è inclusa, con ciò determinando forme di diseguaglianza sociale o discriminazioni verso le minoranze. Alcune categorie di persone, infatti, potrebbero non essere mai raggiunte da alcune offerte, con ciò determinando forme di discriminazione del tutto ingiustificate.

I governi, invece, tendono ad utilizzare la profilazione per prevedere la possibilità che un soggetto sia portato a delinquere.

Inoltre, gli algoritmi di profilazione non sono certamente perfetti, per questo motivo possono portare anche a errori.

Un ulteriore problema è dato dal fatto che gli algoritmi sono protetti quali segreti commerciali (trade secrets), in base alla direttiva Trade Secrets dell'Unione europea e altre norme in materia. In tal senso, quindi, anche i soggetti che utilizzano tali algoritmi, se non ne sono i programmatori, possono non conoscere affatto le logiche alla base degli stessi, e quindi comprendere gli effetti della loro applicazione. Ed ecco perché il regolamento europeo prevede un'apposito obbligo di informazione sulla logica alla base della profilazione.

Violazioni di dati personali (data breach)

L'art. 4 del regolamento europeo definisce la violazione dei dati personali (data breach) come "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".

Quindi, un data breach non è solo un evento doloso come un attacco informatico, ma può essere anche un evento accidentale come un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente). Il nuovo regolamento generale europeo prescrive specifici adempimenti nel caso di una violazione di dati personali.

Notifica della violazione

In base all'art. 33 del GDPR, in caso di violazione dei dati il responsabile del trattamento, se designato, deve avvertire il titolare dell'avvenuta violazione dei dati. Quest'ultimo dovrà, a quel punto, notificare l'evento all'autorità di controllo. tranne che nel caso in cui "sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" (es. perdita di una chiavetta usb con dati cifrati). La notifica deve avvenire "senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza" il titolare. Qualora la notifica non avvenga nelle 72 ore, il titolare dovrà precisare anche i motivi del ritardo.

La norma prevede anche la possibilità di allegare ulteriori informazioni in un momento successivo, per cui è preferibile comunque effettuare la notifica nelle 72 ore, anche se è incompleta.

Contrattualmente titolare e responsabile possono pattuire che la notifica alle autorità spetti al responsabile, sempre per conto del titolare.

Contenuto della notifica

La notifica deve avere il contenuto previsto dall'art. 33 del GDPR:

- 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;

- 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;

- descrivere le probabili conseguenze della violazione dei dati personali;

- 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.

La notifica va effettuata via PEC all'indirizzo protocollo@pec.gpdp.it. L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e opzionalmente la denominazione del titolare del trattamento.

Comunicazione agli interessati

La comunicazione della violazione dei dati agli interessati non è sempre prevista, poiché potrebbe creare un allarme generalizzato e portare ad un danno reputazionale significativo. Per questo si prevede l'obbligo di comunicare la violazione solo se è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Il titolare del trattamento deve comunicare la violazione dei dati all'interessato senza ingiustificato ritardo (art. 34).

L'art. 34 prevede espressamente i casi nei quali non è richiesta tale comunicazione:

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) la 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 analoga efficacia.

Per valutare i fattori che determinano il rischio per le libertà e i diritti degli interessati, il Gruppo di lavoro Articolo 29 (ora EDPB) ha fissato i seguenti parametri:

- tipo di "breach": il tipo di violazione è un parametro per la valutazione del rischio. La violazione dei dati sanitari di tutti i pazienti di un ospedale è ben diversa dalla perdita dei dati sanitari di un singolo paziente;

- natura, numero e grado di sensibilità dei dati personali violati: l'accesso al nome e all'indirizzo dei genitori di un figlio rappresenta un rischio diverso rispetto all'accesso da parte dei genitori naturali del nome e dell'indirizzo dei genitori adottivi;

- facilità di associare i dati violati ad una persona fisica: può accadere che i dati violati non siano facilmente riconducibili ad una determinata persona fisica;

- gravità delle conseguenze per gli Interessati: quando il titolare del trattamento percepisce il rischio che i dati oggetto della violazione possono essere utilizzati immediatamente contro gli Interessati (es. sostituzione di persona);

- numero di Interessati esposti al rischio: un parametro è sicuramente quello del numero degli Interessati potenzialmente coinvolti;

- caratteristiche del titolare del trattamento: un attacco ad una struttura ospedaliera certamente è diverso dall'attacco ad una piccola azienda.

Comunque, 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, con ciò imponendo la comunicazione agli interessati.

La comunicazione agli interessati non deve essere generica, ma deve contenere tutte le informazioni per consentire alle persone di comprendere il riscio e proteggere i loro dati. In particolare dovrà contenere una descrizione della natura della violazione delle sue possibili conseguenze, e dovrà fornire precise indicazioni sugli accorgimenti da adottare per proteggersi da usi illeciti dei primo dati (es. furto di identità) e per evitare ulteriori rischi, Ad esempio potrebbe essere spiegato agli utenti di non utilizzare più le credenziali compromesse e di modificare le password utilizzate per l'accesso ad altri servizi online se uguali o simili a quella violata (Garante Privacy: Provvedimento su data breach - 30 aprile 2019).

Obbligo di documentazione

Il titolare deve documentare le violazioni di dati personali subite, tramite un apposito registro delle violazioni. Il registro dovrà contenere:

- data e ora della violazione;

- sorgente dell'informazione sulla violazione;

- conseguenze della violazione (quantità dei dati personali e degli interessati coinvolti dalla violazione);

- data o ora della notifica della violazione all'autorità di controllo;

- motivo per il quale la violazione è stata ritardata o non è stata comunicata all'autorità di controllo;

- cause della violazione;

- provvedimenti adottati a seguito della violazione.

Tale documentazione dovrà essere fornita al Garante in caso di accertamenti.

Sanzioni

In caso di mancato rispetto delle procedure di notifica della violazione si applica la sanzione amministrativa fino ad un importo di 10 milioni di euro oppure il 2% del fatturato dell'intera società. In caso di mancata notifica si configura anche l'assenza di adeguate misure di sicurezza, per cui si cumulano due distinte sanzioni.

Allegati

- **ALLEGATO 1**: Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007)
- **ALLEGATO 2**: Descrizione delle misure tecniche e organizzative adottate dal fornitore del servizio Registro Elettronico
- **ALLEGATO 3**: Descrizione delle misure tecniche e organizzative adottate dal fornitore del servizio di dematerializzazione Segreteria Digitale