LICEO STATALE "Angela Veronese"
Artistico - Economico Sociale - Linguistico - Scienze Umane
Viale della Vittoria 34 - 31044 MONTEBELLUNA (Treviso)
Tel. 0423 601752 - **Fax** 0423 601970 - **C.F.** 83005990268 - **C.M.** TVPM02000G
email TVPM02000G@istruzione.it - **sito web** www.liceoveronese.edu.it
email pec TVPM02000G@pec.istruzione.it

POLICY PRIVACY
REGOLAMENTO D'ISTITUTO

INFORMAZIONI DOCUMENTO:

Titolo	Regolamento d'Istituto Privacy		
Data di emissione	13.01.2021	**Versione**	A513000.05.00 rev. 02

SOMMARIO

PARTE PRIMA: INTRODUZIONE 4

1. PREMESSA DI CARATTERE NORMATIVO 4
2. PREMESSA DI CARATTERE ORGANIZZATIVO 4
3. PREMESSA DI CARATTERE METODOLOGICO 5

PARTE SECONDA: DISPOSIZIONI GENERALI 6

4. OGGETTO DEL REGOLAMENTO 6
5. FINALITA' DEL REGOLAMENTO 6
6. SENSIBILIZZAZIONE 6
7. DEFINIZIONI 7
8. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI 8
9. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI) 9
10. TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI) 9
11. COMUNICAZIONE DI DATI VERSO L'ESTERNO 10

PARTE TERZA: DIRITTI DELL'INTERESSATO 11

12. INFORMATIVA SUL TRATTAMENTO DEI DATI 11
13. CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI 12
14. DIRITTO DI ACCESSO DELL'INTERESSATO 12
15. DIRITTO DI RETTIFICA 13
16. DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO) 13
17. DIRITTO DI LIMITAZIONE AL TRATTAMENTO 13
18. DIRITTO ALLA PORTABILITA' DEI DATI 14
19. DIRITTO DI OPPOSIZIONE 14
20. PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE) 14

PARTE QUARTA: DIRITTI DI ACCESSO AGLI ATTI DELL'ISTITUTO 15

21. ACCESSO AGLI ATTI 15

PARTE QUINTA: TITOLARE E RESPONSABILE DEL TRATTAMENTO 17

22. TITOLARE DEL TRATTAMENTO 17
23. CONTITOLARI DEL TRATTAMENTO 17
24. DELEGATO DEL TRATTAMENTO DEI DATI 18
25. RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI EX ART. 28 DEL GDPR 19
26. AUTORIZZATO AL TRATTAMENTO DEI DATI 20
27. RESPONSABILE DELLA PROTEZIONE DEI DATI 21

PARTE SESTA: SICUREZZA DEI DATI PERSONALI - MISURE DI CARATTERE INFORMATICO E TECNOLOGICO 23

28. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA 23
29. REGISTRO ELETTRONICO DELLE ATTIVITA' DI TRATTAMENTO 23
30. PROTEZIONE E SICUREZZA DEI DATI PERSONALI 23
31. NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO 24
32. VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI 24
33. TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO 25
34. DISCIPLINA AZIENDALE SULLA VIDEOSORVEGLIANZA ..... **Errore. Il segnalibro non è definito.**
PARTE SETTIMA: ATTUAZIONE DEGLI ADEMPIMENTI EUROPEI 26
35. ENTRATA IN VIGORE E PUBBLICITA' 26
36. DISPOSIZIONE FINALE RELATIVA AGLI 'ALLEGATI TECNICI' 26
A. REGOLE PER L'ADOZIONE DELLE MISURE DI SICUREZZA 27
B. ISTRUZIONI OPERATIVE SULLE CORRETTE MODALITÀ DI UTILIZZO DEGLI STRUMENTI IN SMART WORKING 30
C. DISCIPLINARE PER L'AUTORIZZATO AL TRATTAMENTO 35
D. PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI – DATA BREACH 37

PARTE PRIMA: INTRODUZIONE

1. PREMESSA DI CARATTERE NORMATIVO

Il presente Regolamento in materia di protezione dei dati personali (così detta “privacy”) è uno strumento di applicazione del vigente Decreto Legislativo 30 giugno 2003, n. 196 (cosiddetto "Codice sulla privacy”) e, in particolare, del nuovo **Regolamento Europeo n. 2016/679**, nell'ambito dell'organizzazione dell’Istituto Liceo "A. Veronese".

Dal 25 maggio 2018 ha trovato diretta applicazione, sul territorio nazionale, il nuovo Regolamento Europeo sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell’Unione Europea il 04 maggio 2016.

Il Regolamento disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.

In data 19/09/2018 è entrato in vigore il Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.

E’ necessario pertanto, come Istituto, dotarsi sin da ora di un apposito “Regolamento” che disciplini compiti, attività e *policy* interne che garantiscano l’assolvimento degli adempimenti imposti dalle norme europee.

Il presente Regolamento d’Istituto si rende inoltre necessario per recepire, in un unico testo, i precetti normativi di maggior rilevanza, sia di carattere istituzionale che nazionale in tema di trattamento dei dati personali *(D.lgs. 196 del 30/06/2003 e ss.mm., regolamenti e codici deontologici succeduti negli ultimi anni, direttive e linee guida del Garante, Direttiva dell'UE 2000/58 sulla riservatezza nelle comunicazioni elettroniche e soprattutto Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).*

Il presente Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

2. PREMESSA DI CARATTERE ORGANIZZATIVO

Un’ attenta disamina della normativa vigente in materia di privacy ha fatto emergere una necessità imprescindibile di cambiamento della mentalità che porti alla piena tutela della stessa, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-utente che si rivolge all’Istituto, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla privacy costituisce, anche secondo il Legislatore Europeo, un vero e proprio diritto inviolabile dell’essere umano, che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali nonché dignità del singolo individuo. Per questi motivi, la “cultura della privacy” necessita di divenire un vero e proprio elemento cardine dell’organizzazione di questo Istituto. A tale scopo è necessario che L’Istituto per mezzo del proprio personale si adoperi affinchè possa crescere e rafforzarsi una maggiore consapevolezza in materia e ciò, non solo con una conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa nel trattamento dei dati, ma anche ponendo in essere tutti gli adempimenti di carattere tecnico ed organizzativo per contribuire concretamente al miglioramento della qualità del rapporto con l'utenza.

3. PREMESSA DI CARATTERE METODOLOGICO

Vengono allegati a questo Regolamento una serie di **documenti tecnici** atti a dare compiuta attuazione ai dettami della nuova "privacy europea".

Tali documenti, ai quali viene data massima pubblicità e diffusione tramite la pubblicazione sul sito *internet* dell'istituto, sono:

A. Regole per l'adozione delle misure di sicurezza;
B. Disciplinare per l'uso della rete informatica;
C. Regolamento per il lavoro agile "smart working"
D. Disciplinare per l'autorizzato al trattamento;
E. Procedura per la gestione delle violazioni – data breach;

Si sottolinea come il principio cardine della "responsabilizzazione" (accountability nell'accezione inglese), introdotto dal nuovo Regolamento UE, imponga al Titolare del trattamento dei dati l'obbligo di attuare delle politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della **"conformità"** o ***compliance*** nell'accezione inglese); ciò anche attraverso dei comportamenti proattivi, atti a dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

La normativa vigente lascia al Titolare ampia autonomia decisionale in merito alle modalità, alle garanzie e ai limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Pertanto questo Istituto si sta impegnando, a far propri i dettami del Legislatore europeo relativi all'*accountability* ed alla *compliance*. anche attraverso la predisposizione di questo documento.

PARTE SECONDA: DISPOSIZIONI GENERALI

4. OGGETTO DEL REGOLAMENTO

Il presente Regolamento disciplina, all'interno dell'Istituto, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali (Decreto Legislativo del 30/06/2003 n. 196 e ss.mm.) ed in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE n. 679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi.

5. FINALITA' DEL REGOLAMENTO

Il presente Regolamento ha come fine quello di modulare la gestione dei Dati con criteri e procedure unitarie, volte alla massima tutela delle persone fisiche alle quali gli stessi si riferiscono.
L'Istituto, in virtù di quanto suddetto pertanto, garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della *Carta dei diritti fondamentali* dell'Unione Europea.)

6. SENSIBILIZZAZIONE

Il Liceo "A. Veronese" sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto agli studenti e ai loro familiari.
A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale dell'Istituto e l'attività informativa diretta a tutti coloro che hanno rapporti con lo stesso.
Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento Europeo, e di conseguenza contenute nel presente Regolamento , al momento dell'ingresso in servizio è fornita, a cura dell'Ufficio Personale, ad ogni dipendente *(oltre che ad ogni collaboratore, consulente)* una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro *(o nella lettera di incarico per i soggetti non dipendenti poc'anzi citati)*, con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali **"autorizzati al trattamento dei dati"** e **"responsabili esterni al trattamento"** ai sensi del Regolamento UE 2016/679.
Il Regolamento, pubblicato sul sito Istituzionale, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

7. DEFINIZIONI

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare d'istituto si intende per:

a) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può esser 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) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

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) «**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;

f) «**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;

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) «**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;

l) «**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;

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) «**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;

o) «**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; a proposito delle tipologie di "dati" sopra indicate, si fa presente che il Regolamento europeo non utilizza la definizione ***"dati sensibili"*** per la quale, quanto meno sino all'emanazione della legge italiana di revisione del D.lgs. 196/20013, si fa espresso rinvio all'articolo n. 4 del vigente Codice della privacy (D.lgs. 196/2003): definizione che, quindi, al momento rimane nell'utilizzo e nel linguaggio corrente per la materia di cui si tratta.

p) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679.

8. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 5 del Regolamento Europeo n. 2016/679, i dati personali sono:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato *(«**liceità, correttezza e trasparenza**»);*

b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali *(«**limitazione della finalità**»);*

c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati *(**«minimizzazione dei dati»**).* A tale proposito, il Regolamento UE ricalca i principi sostanziali di ***"necessità, pertinenza, indispensabilità e non eccedenza"*** (rispetto alle finalità del trattamento) contenuti negli articoli 4 e 11 del D.lgs. 196/2003.

d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati *(«**esattezza**»);*

e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva

l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato *(«**limitazione della conservazione**»);*

f. 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**»).*

Come stabilito dal Regolamento UE, il Titolare del trattamento è competente per il rispetto di quanto sin qui esposto ed è in grado di comprovarlo verso l'esterno (principio europeo dell'*«**accountability**»* o *«**responsabilizzazione**»).*

9. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'*origine razziale o etnica*, le *opinioni politiche*, le *convinzioni religiose* o *filosofiche*, o *l'appartenenza sindacale*, nonché trattare *dati genetici, dati biometrici* intesi a identificare in modo univoco una persona fisica, *dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*.

Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato articolo n. 9, tra le quali si evidenzia quella di cui alla lettera "g" applicabile a questo Istituto, ai sensi della quale "*il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*

Si fa presente, inoltre, che il Regolamento UE consente di *"mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute"* (articolo n. 9, paragrafo n. 4).

Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati sensibili, biometrici e genetici e in particolare al "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art.21, comma 1 del D.Lgs. 10 Agosto 2018, n. 101" del Garante della Privacy, pubblicato in Gazzetta Ufficiale il 05 Giugno 2019.

10. TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679, *"il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica."*

Il Regolamento UE 2016/679 pertanto ravvisa quali condizioni necessarie per il trattamento suddetto la presenza di una base giuridica che lo giustifichi (l'art. 6, paragrafo 1 del GDPR) ed altresì il controllo dell'autorità pubblica o l'autorizzazione del diritto dell'Unione o degli Stati membri, nel rispetto delle garanzie appropriate per i diritti e le libertà degli interessati.

Sul tema si sottolinea come la dottrina prevalente, in merito al fondamento giuridico che consenta di trattare i dati relativi a condanne penali e reati per valutare l'attitudine lavorativa, ha ritenuto che l'autorizzazione da parte del diritto nazionale già risulti presente ai sensi dell'art. 8 del c.d. "Statuto dei Lavoratori" (L. 300/1970) che ne prevede il trattamento nell'ambito della valutazione dell'attitudine lavorativa.

11. COMUNICAZIONE DI DATI VERSO L'ESTERNO

La comunicazione a soggetti terzi di dati di carattere personale e particolare, detenuti dal Titolare del Trattamento, deve avvenire unicamente in ragione delle finalità per le quali gli stessi sono stati acquisiti e di cui si è data contezza nell'informativa privacy consegnata e sottoscritta dagli interessati.

La diffusione di dati che ecceda quanto su indicato, deve considerarsi illecita.

L'eventuale **comunicazione di dati particolari e giudiziari tra soggetti pubblici,** è ammessa solo in presenza di una normativa o di un regolamento che la giustifichino e, in ogni caso, qualora risulti necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi.

PARTE TERZA: DIRITTI DELL'INTERESSATO

12. INFORMATIVA SUL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti **informazioni:**

a. l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b. i dati di contatto del Responsabile della protezione dei dati (D.P.O.);
c. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d. qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f. ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti **ulteriori informazioni necessarie** per garantire un trattamento corretto e trasparente:

g. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
h. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al *diritto alla portabilità* dei dati;
i. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
j. il diritto di proporre reclamo a un'autorità di controllo;
k. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
l. l'eventuale esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questo Istituto, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tale riguardo, sia fa rinvio al **massimario di conservazione e scarto in uso presso l'Istituto.**

Per massimario di conservazione e di scarto si intende l'elenco della tipologia dei documenti con il rispettivo tempo di conservazione (limitato o illimitato); detto strumento permette di gestire in modo organizzato l'archivio d'Istituto,

permettendo di conservare solo ciò che mantiene un rilievo giuridico o ha assunto un valore storico e di eliminare la documentazione non più necessaria.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una **finalità** diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.

13. CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

Il consenso al trattamento dei dati rappresenta la base giuridica che consente all'Ente di trattare i dati dell'interessato ogni qualvolta il trattamento non possa trovare giustificazione in basi giuridiche più specifiche, le quali vengono espressamente previste agli artt. 6 e 9 del GDPR.

- Per permettere che il trattamento di dati basato sul consenso possa considerarsi lecito è necessario che questo presenti dei requisiti che di seguito si esplicano: **il consenso deve essere "esplicito"** o il trattamento deve basarsi sul verificarsi dei casi previsti dal GDPR;
- deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile** e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare "caselle pre-spuntate" su un modulo);
- deve essere manifestato attraverso **"dichiarazione o azione positiva inequivocabile"** (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

14. DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere **l'accesso** ai dati personali e alle seguenti informazioni:

a. le finalità del trattamento;
b. le categorie di dati personali in questione;
c. i destinatari 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;
d. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f. il diritto di proporre reclamo a un'autorità di controllo;
g. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h. l'esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo diritto, il Titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

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 ai sensi dell'articolo 46 relative al trasferimento.
Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.
In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

15. DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

16. DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 2016/679, in capo all'interessato è riconosciuto il **diritto "all'oblio",** che si configura come un diritto alla cancellazione dei propri dati personali **in forma rafforzata.**
Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento UE).
Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice della privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda articolo 17, paragrafo 1).

17. DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì **anche se l'interessato chiede la rettifica dei dati** *(in attesa di tale rettifica da parte del titolare)* **o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento** *(in attesa della valutazione da parte del titolare).*
Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la **limitazione** è vietato a meno che ricorrano determinate circostanze *(consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).*
Il diritto alla limitazione prevede che il dato personale sia **"contrassegnato"** in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

18. DIRITTO ALLA PORTABILITA' DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste **specifiche condizioni per il suo esercizio**; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al Titolare (si veda il considerando 68 del Regolamento UE).

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

19. DIRITTO DI OPPOSIZIONE

Come stabilito dall'articolo n. 21 del Regolamento Europeo n. 2016/679, 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 ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, 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.

20. PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

Come stabilito dall'articolo n. 22 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul **trattamento automatizzato**, compresa la **profilazione,** che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

PARTE QUARTA: DIRITTI DI ACCESSO AGLI ATTI DELL'ISTITUTO

21. ACCESSO AGLI ATTI

L'utenza può esercitare anche i diritti connessi all'accesso agli atti e documenti dell'Istituto, mediante lo strumento di accesso agli atti.

A tale riguardosi fa presente che:

a. per ***accesso documentale*** si intende la domanda di accesso (richiesta di presa visione o di rilascio copia) a delibere e provvedimenti dell'Istituto, nei termini e alle modalità previste dalla normativa vigente (Legge 07 agosto 1990 n. 241 e ss.mm.ii. e D.P.R. 12 aprile 2006 n. 184). Possono fare domanda tutti i cittadini portatori di un interesse *"diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso"* (art. 22, Legge 241/1990). Tali termini sono sospesi (fino ad un massimo di 10 giorni) nel caso di comunicazione della richiesta al controinteressato il quale ha diritto di presentare le proprie opposizioni. Il procedimento di accesso si conclude entro 30 giorni, decorrenti dalla presentazione della richiesta all'ufficio competente (art. 6 del D.P.R. 184 del 2006).

b. per ***accesso civico*** si intende il diritto di chiunque di richiedere documenti, informazioni o dati che le pubbliche amministrazioni non hanno pubblicato pur avendone l'obbligo (Decreto Legislativo 97 del 17/5/2016 *"Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza delle Amministrazioni Pubbliche*", e Decreto Legislativo 33 del 14/03/2013: *"Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"*). L'Istituto, entro 30 giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, l'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, l'Istituto indica al richiedente il relativo collegamento ipertestuale. Nei casi di ritardo o mancata risposta il richiedente può ricorrere al titolare del potere sostitutivo (indicato sul sito web istituzionale) che, verificata la sussistenza dell'obbligo di pubblicazione, provvede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto.

   per ***accesso generalizzato*** si intende il diritto di chiunque di accedere ai dati e ai documenti detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del Decreto Legislativo 33/2013 ('Decreto Trasparenza') e del D.lgs. 97/2016 (così detto *Freedom of Information Act* o "FOIA"), nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico

   Il procedimento di accesso generalizzato deve concludersi con provvedimento espresso e motivato nel termine di 30 giorni dalla presentazione dell'istanza. Se il documento risulta già pubblicato nel sito istituzionale nel rispetto della normativa vigente, l'Istituto indica al richiedente il relativo collegamento ipertestuale. Nei casi di diniego totale o

parziale dell’accesso o di mancata risposta entro il termine indicato, il richiedente può presentare richiesta di riesame all’Istituto, che decide con provvedimento motivato, entro il termine di 20 giorni. Avverso la decisione dell’amministrazione competente, il richiedente può proporre ricorso al tribunale amministrativo regionale (TAR).

Le richieste dovranno essere presentate con le modalità riportate nello specifico Regolamento di istituto per l'accesso.

PARTE QUINTA: TITOLARE E RESPONSABILE DEL TRATTAMENTO

22. TITOLARE DEL TRATTAMENTO

Il ***"Titolare"*** del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti della vigente normativa in materia di privacy, è il Liceo "A. Veronese" di Montebelluna.

Il Titolare, avvalendosi della supervisione e collaborazione del ***Data Protection Officer***, provvede:

a. a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;
b. a nominare con atto deliberativo i *Responsabili del trattamento dei dati personali,* impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy e all'articolo 12 del Regolamento UE, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
c. a nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE;
d. a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
e. a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

Si dà evidenza, inoltre, del fatto che il Regolamento UE pone con forza l'accento sulla **"responsabilizzazione"** (***accountability*** nell'accezione inglese) di titolari e responsabili, ovverossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del Regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Questo Istituto sta lavorando attivamente per far proprio l'approccio del Legislatore europeo relativo all'*accountability*.

23. CONTITOLARI DEL TRATTAMENTO

Come stabilito dall'articolo n. 26 del Regolamento Europeo n. 2016/679, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono **contitolari del trattamento.** Essi determinano in modo trasparente, mediante un *accordo interno,* le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

24. DELEGATO DEL TRATTAMENTO DEI DATI

Secondo il D.lgs. 196/2003, s'intende per Responsabile del trattamento dei dati, *"la persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altra Associazione ed Organismo preposti dal Titolare al trattamento di dati personali".*
Anche se il Regolamento Europeo (art. 28) disciplina i compiti del Responsabile "esterno" senza contemplare espressamente la figura ed i compiti del Responsabile "interno".
Questo Istituto, in considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di continuare a garantire, a tutti i livelli, la più efficace applicabilità dei precetti in materia di privacy, reputa necessario, come sempre avvenuto in passato, continuare a designare i ***Delegati del trattamento dei dati personali,*** conferendo l'incarico a quei soggetti apicali che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.
In base all'organizzazione di questo Istituto vengono individuati quali **Delegati del trattamento dei dati personali, le seguenti figure professionali**

- DSGA

Il Titolare del trattamento dei dati deve informare ciascun delegato del trattamento dei dati, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti.
I delegati del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

Il Delegato del trattamento deve:

1. trattare i dati personali, anche sensibili, osservando le disposizioni del presente Regolamento d'istituto nonché le specifiche istruzioni impartite dal Titolare;
2. garantire che, presso la propria struttura, le persone autorizzate (incaricate) al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza;
3. adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;
4. tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;
5. mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel presente Regolamento;
6. contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

Il delegato al trattamento dei dati personali, nell'espletamento della sua funzione, deve inoltre collaborare con il **Data Protection Officer (DPO)**, al fine di:

a. comunicare al DPO, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE 2016/679 riguardanti: *l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato, la predisposizione del Registro dei trattamenti*.

b. utilizzare il modello d'Istituto di *Informativa e Consenso*, verificandone il rispetto e fornendo al DPO, quando questi ne faccia richiesta, le informazioni utili per l'aggiornamento del registro dei trattamenti;

c. rispondere alle istanze degli interessati secondo quanto stabilito dal Codice della privacy e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;

d. contribuire a far sì che tutte le misure di sicurezza riguardanti i dati dell'Istituto siano applicati al suo interno ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;

e. informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

Questo Istituto ha provveduto alla **nomina dei Delegati del trattamento dei dati**, mediante apposito atto di nomina.

25. RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI EX ART. 28 DEL GDPR

Nell'ambito di questo Istituto, sono inoltre individuati quali **Responsabili del trattamento dei dati personali**, tutti i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto sottoscritto con l'Istituto, trattino dati di cui lo stesso è titolare e qualora siano in possesso dei requisiti previsti dall'articolo 28 del Regolamento EU (esperienza, capacità ed affidabilità).

In ottemperanza all'articolo 28 del Regolamento Europeo 2016/679, i Responsabili hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;
- trattare i dati personali, anche di natura sensibile e giudiziaria, degli interessati esclusivamente per le finalità previste dal contratto o dalla convenzione stipulata con il Liceo "A. Veronese" e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;
- rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
- adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento Europeo 2016/679 rubricato "Sicurezza del trattamento" che possono anche essere definite dal Titolare del Trattamento;
- nominare, al loro interno, i soggetti autorizzati / incaricati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;

- attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;
- specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.
- assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo *(sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati),* tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento Europeo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

La nomina di Responsabile esterno del Trattamento avviene mediante la sottoscrizione di un contratto che integra gli accordi/convenzioni/contratti che regolano i rapporti principali in essere tra le parti.

La sottoscrizione del contratto di nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.

26. AUTORIZZATO AL TRATTAMENTO DEI DATI

Il Regolamento Europeo non fornisce rilievo autonomo alla figura dell'*incaricato* al trattamento dei dati, seppure si soffermi sul fatto che chi tratta dati, ricevendo istruzioni e formazione da parte del Titolare del trattamento debba da questi essere *"autorizzato"* al trattamento (articoli 4 e 10 del Regolamento).

Come già stabilito all'articolo 6 del presente Regolamento, al momento dell'ingresso in servizio è fornita, a cura dell'ufficio di competenza, ad ogni dipendente *(oltre che ad ogni collaboratore, consulente o titolare di borsa di studio)* una specifica documentazione in materia di privacy all'interno della quale è presente anche l'atto di nomina ad autorizzato al trattamento dei dati.

La nomina di autorizzato, costituisce un atto unilaterale ricettizio di cui il dipendente deve solo prendere atto; la non volontà di accettazione della nomina non permette l'instaurazione del rapporto lavorativo.

Solo attraverso la nomina di autorizzato al trattamento infatti, il dipendente può visionare, trattare e gestire i Dati detenuti dall'Istituto.

Contestualmente alla nomina dovrà essere data copia del presente Regolamento o, in alternativa, indicazioni per poterla scaricare dal sito internet dell'Istituto.

Il Regolamento contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di autorizzato), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.
La nomina di autorizzato al trattamento è valevole anche per le figure professionali che collaborano con l'Istituto, anche se non alle dirette dipendenze dello stesso, e che, in virtù di detta attività, possono accedere e trattare Dati stando però alle direttive dello stesso.
Ci si riferisce, a titolo esemplificativo, al *personale tirocinante* o al *personale volontario* che opera temporaneamente all'interno dell'Istituto in virtù di un accordo o di una convenzione per lo svolgimento, appunto, di tirocini formativi piuttosto che di attività di volontariato a sostegno degli alunni, dei loro genitori e del personale dell'Istituto.
Il personale di cui si parla è soggetto agli stessi obblighi cui sono sottoposti tutti gli autorizzati "interni", in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.
Nel caso di Autorizzati "*esterni*", l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

27. RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Regolamento Europeo impone la nomina del ***Data Protection Officer*** (DPO, in italiano: Responsabile della protezione dei dati o 'RDP'), nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.
Chi svolge la funzione di RPD deve aver conseguito un percorso accademico- lavorativo volto alla precisa e puntuale conoscenza della normativa e delle procedure legate alla protezione dei dati personali oltre che presentare caratteristiche di indipendenza ed autorevolezza.
Il Regolamento Ue sottolinea l'importanza del requisito di indipendenza richiesto a tale figura, pertanto risulta evidente che il DPO non deve essere in **conflitto di interessi con l'Ente per cui presta la propria assistenza.**
Il Liceo "A. Veronese" provvede al conferimento dell'incarico di cui si tratta, tenendo conto delle prescrizioni sin qui descritte.
Ai sensi dell'articolo 39 del Regolamento UE, i suoi compiti sono:

- **sorvegliare l'osservanza del Regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;
- **fornire consulenza e pareri** al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
- collaborare con il titolare, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA);**
- **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- **cooperare con il Garante e fungere da punto di contatto per il Garante** su ogni questione connessa al trattamento;
- **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento**.

Ai sensi dell'articolo 37 del Regolamento UE, Egli deve:

- **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;
- **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse.** In linea di principio, ciò significa che il RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;
- **operare alle dipendenze del titolare oppure sulla base di un contratto di servizio** (RPD esterno);
- **disporre di risorse umane e finanziarie**, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il Regolamento UE prevede la pubblicazione *on line* del curriculum del RDP, nonché la pubblicazione sul sito istituzionale dell'Istituto dei **"dati di contatto" del RDP**: dati che debbono essere inseriti anche nell'informativa istituzionale sul trattamento dei dati, così che il RDP sia agevolmente contattabile dai cittadini-utenti ma anche dal Garante per la privacy.

Sia che il RDP sia interno che esterno, è necessario stipulare con il medesimo un **contratto ad hoc.** Nel caso in cui il RDP sia un "esterno" (persona o società) tutte le clausole, oltre che il compenso per l'incarico, dovranno essere inserite in un apposito contratto di servizi, ove siano anche previste le risorse necessarie a far funzionare l'ufficio del RDP.

PARTE SESTA: SICUREZZA DEI DATI PERSONALI - MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

28. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese ***"data protection by default and by design"***, ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (*"sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso",* secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

29. REGISTRO ELETTRONICO DELLE ATTIVITA' DI TRATTAMENTO

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un **registro delle operazioni di trattamento** i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un Istituto, indispensabile per ogni valutazione e analisi del rischio.

Il Registro deve essere esibito su richiesta del Garante.

La tenuta del registro dei trattamenti costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

30. PROTEZIONE E SICUREZZA DEI DATI PERSONALI

Le misure di sicurezza devono ***"garantire un livello di sicurezza adeguato al rischio***" del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Per lo stesso motivo, secondo il Regolamento UE non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Il 05 Giugno 2019 il Garante della Privacy ha emanato il "*Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.Lgs. 10 agosto 2018 n.101*" contenente le indicazioni specifiche per alcune fattispecie di trattamenti.

31. NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO

A partire dal 25 maggio 2018, tutti i titolari dovranno **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque *"senza ingiustificato ritardo",* ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del Regolamento UE); questa procedura va sotto il nome di ***"Data Breach".***

Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre *"senza ingiustificato ritardo";* fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento, nonché dalle "*Linee Guida in materia di notifica delle violazioni di dati personali – WP250, definite in base alle previsioni del Regolamento UE 2016/679*" adottate dal Gruppo di Lavoro Art.29 il 03 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) e dal Provvedimento del Garante sulla notifica delle violazioni dei dati personali del 30 Luglio 2019.

Il Titolare del trattamento, sentito il Data Protection Officer, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Si ricorda, inoltre, che l'Autorità ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico

(https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=1.1).

32. VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI

L'Istituto adotta le misure atte a ***"garantire un livello di sicurezza adeguato al rischio***" del trattamento (articolo 32, paragrafo 1 del Regolamento UE) e ciò sulla base di quanto disposto dall'art 32, par. 1 del GDPR, che costituisce la base operativa su cui attuare la prevenzione.

fra le attività correlate alla sicurezza, di fondamentale importanza per questo Istituto sono le misure collegate al, al **rischio inerente al trattamento.**

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77 del GDPR); tali impatti dovranno essere analizzati attraverso un apposito **processo di valutazione** (si vedano artt. 35-36 del GDPR) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All'esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

33. TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Si fa rinvio ai principi dettati dal Regolamento Europeo agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali.

PARTE SETTIMA: ATTUAZIONE DEGLI ADEMPIMENTI EUROPEI

34. ENTRATA IN VIGORE E PUBBLICITA'

Il Regolamento è in vigore dalla data di approvazione, mediante delibera espressa del Consiglio di Istituto.
Il Regolamento è pubblicato nel sito internet dell'Istituto nell'apposita sezione dedicata alla "privacy europea".

35. DISPOSIZIONE FINALE RELATIVA AGLI 'ALLEGATI TECNICI'

Il testo del presente Regolamento potrà essere aggiornato con atto deliberativo del CdI, a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, sia nazionale che regionale, in materia di protezione dei dati personali.
Quanto, invece, ai n. [4] (quattro) **Allegati tecnici** al presente Regolamento, si stabilisce quanto segue: poiché si tratta di "strumenti di lavoro quotidiano", essi saranno inevitabilmente oggetto di continue, quanto rapide integrazioni, modifiche e revisioni, in virtù sia delle necessità che delle esigenze imposte da una realtà normativa ed organizzativa tuttora in rapidissima evoluzione.
Gli eventuali aggiornamenti ai *documenti tecnici allegati* verranno, pertanto, inseriti in tempo reale sul sito internet istituzionale nell'apposita sezione dedicata alla "privacy", prescindendo dall'adozione di appositi atti deliberativi di modifica del presente Regolamento e dandone pubblicità per mezzo di apposita circolare così da consentire una rapida consultazione on line dei medesimi ed un contenuto sempre aggiornato degli stessi.

A. REGOLE PER L'ADOZIONE DELLE MISURE DI SICUREZZA

Le misure di sicurezza che l'Istituto adotta, vengono valutate sulla base de rischio e del contesto ambientale, così come dettato dall'art. 32 del GDPR, il quale espressamente dispone "*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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*

Si riportano, a titolo esemplificativo, le misure di sicurezza che l'Istituto intende implementare sulla base di specifici principi e regole per la loro applicabilità.

Misure	**Regole / Principi da osservare**
Presenza di un sistema di allarme	E' importante che l'Istituto si doti di impianto d'antifurto a tutela del patrimonio delle informazioni contenute al suo interno.
Custodia dei dati in armadi blindati e/o ignifughi	E' importante che gli uffici che trattano dati sensibili e giudiziari possano disporre di queste strutture per archiviare in modo consono tali informazioni.
Sistemi UPS e Generatori di corrente che garantiscano la continuità elettrica	Fondamentale a tutela delle attività soprattutto per gli strumenti elettronici. Da adottare necessariamente per tutti i server e per quei pc locali che non archiviano le informazioni sul server. Infatti questi ultimi non hanno delle procedure pianificate di backup e quindi è importante ridurre al minimo i rischi che gli sbalzi di tensione possono provocare sugli hard disk.
Digitazione password all'accensione del PC	Tutti i PC devono avere la password di Windows all'accensione del terminale, questo non vale solo come regola ma viene considerata una misura base di sicurezza.
Manutenzione programmata degli strumenti	Come tutte le macchine che si rispettano anche il sistema informativo va manutenzionato periodicamente sia attraverso l'aggiornamento dei suoi componenti sia con la pulizia periodica delle macchine stesse.
Utilizzo di un sistema firewall	Obbligatorio viste le forme di attacco sempre più intelligenti.
Presenza di un sistema di autenticazione delle credenziali per tutti gli accessi agli archivi elettronici	Si intende con questa misura l'adozione di un server di dominio che consenta l'autenticazione dell'utente.

Disattivazione delle credenziali di autenticazione nel caso di inutilizzo per 6 mesi	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Controllo degli accessi a siti internet non sicuri – Protezione della posta elettronica	E' importante la conoscenza da parte degli operatori della navigazione in internet e dell'uso della posta elettronica. A questo proposito è stato introdotto il regolamento per l'uso del PC.
Utilizzo di un filtro anti-spam	All'interno dello spam (posta indesiderata) si annidano spesso dei fenomeni di illegalità informatica. E' importante dotare l'Istituto di tale strumento
Utilizzo di un antivirus	Per quanto precedentemente detto, è importante la presenza di un antivirus in ogni posto di lavoro, considerata misura di sicurezza e ovviamente che sia aggiornato
Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durante le sessioni di lavoro	E' importante che l'operatore conosca il regolamento per quanto concerne l'assenza dal posto di lavoro con il PC acceso.
Disattivazione delle credenziali di autenticazione in caso di perdita di qualità dell'incarico	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Aggiornamento periodico, con cadenza almeno annuale, della lista degli incaricati e dei profili di autorizzazione	Tutte le persone che operano all'interno degli uffici devono essere autorizzate dal Titolare
Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione	Rientra nel concetto della formazione del personale
Aggiornamento periodico delle credenziali di autenticazione	Spetta all'incaricato della custodia delle password disattivare le credenziali che hanno perso efficacia
Procedure di verifica sull'operato degli incaricati	E' un compito ispettivo che il Responsabile della sicurezza dei dati personali può demandare anche a società esterne
Formazione sugli aspetti principali della disciplina della privacy al momento dell'ingresso in servizio	Rientra nel concetto della formazione del personale
Formazione, periodica e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti per il trattamento dei dati e la loro protezione	Rientra nel concetto della formazione del personale

Istruzioni finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento	Rientra nel concetto della formazione del personale
Adozione di procedure per le copie di sicurezza, la loro custodia ed il ripristino della disponibilità dei dati	Il backup dei dati trattati dagli uffici amministrativi essere metodico, non affidato alle singole volontà. E' per questo importante nominare l'Incaricato delle copie di sicurezza delle banche dati
Definizioni di responsabilità e sanzioni disciplinari	Rientra nel concetto della formazione del personale nonché è necessario integrare il codice di comportamento includendo sanzioni disciplinari nei casi in cui ci sia un comportamento difforme da quando indicato dal presente Regolamento
Formazione professionale	Rientra nel concetto della formazione del personale
Distruzione del cartaceo	E' importante nel limite del possibile incentivare la distruzione del cartaceo rendendolo illeggibile usando dei comodi distruggi documenti. In assenza di tali strumenti, sarà cura del singolo dipendente provvedere alla distruzione manuale in modo che lo stesso non possa essere facilmente ricostruibile.
Per accedere sono attive le credenziali di autenticazione	Questa misura comporta, per gli uffici amministrativi, l'adozione di un server di dominio che consenta l'autenticazione dell'utente
Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati	Il salvataggio dei dati è fondamentale in qualsiasi organizzazione
I dati cartacei sono chiusi in un armadio	Ogni documento deve essere possibilmente chiuso in un armadio. Qualora questo non possa essere possibile, sicuramente che possano essere chiusi i dati sensibili e quelli giudiziari

B. ISTRUZIONI OPERATIVE SULLE CORRETTE MODALITÀ DI UTILIZZO DEGLI STRUMENTI IN SMART WORKING

1. Premesse e applicazione

Con il presente regolamento il Liceo "A. Veronese" intende disciplinare le norme comportamentali che tutto il personale in servizio, autorizzato ad operare in modalità smart working, deve rispettare.

Per quanto non previsto in questo documento, si richiamano comunque nel loro complesso le norme di legge, compreso quanto previsto dal contratto collettivo nazionale di lavoro riguardanti i doveri dei lavoratori.

Le presenti istruzioni hanno come scopo quello di indicare le misure organizzative aventi l'obiettivo di proteggere tutti i dati trattati dall'Istituto.

Divieto di comunicazione e divulgazione

È fatto assoluto divieto di comunicazione e divulgazione di qualsivoglia dato che l'incaricato è autorizzato a trattare, se non previa autorizzazione del proprio responsabile, il quale, in caso di dubbio o di situazioni particolarmente delicate, può rivolgersi direttamente al datore di lavoro, che darà eventuale autorizzazione. Tale divieto si intende esteso anche al periodo successivo alla scadenza dell'incarico o del rapporto di lavoro e comunque sino a quando le suddette informazioni non vengano divulgate ad opera del datore di lavoro oppure divengano di dominio pubblico.

2. Istruzioni per il corretto trattamento dati con strumenti informatici forniti dall'Istituto

Utilizzo degli strumenti istituzionali

Come è noto, gli strumenti di lavoro sono sotto la responsabilità dell'Istituto stesso, che li mette a disposizione dei propri addetti alle seguenti condizioni:

- gli strumenti possono essere utilizzati solo per fini istituzionali (in relazione alle mansioni assegnate);
- gli strumenti vengono custoditi con cura dal lavoratore cui sono assegnati, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti;
- vengono sempre rispettate le presenti istruzioni e le norme di buon comportamento.

Utilizzo di telefono mobile

In sede di consegna di un telefono cellulare, smartphone, tablet o simili, il datore di lavoro ne disciplina l'uso per eventuale finalità diversa dall'esecuzione delle prestazioni lavorative.

Si precisa comunque che il dispositivo è e resta di proprietà dell'Istituto, che ha facoltà di esercitare in qualsiasi momento ogni diritto previsto dalle disposizioni legislative vigenti.

I dipendenti e i collaboratori sono responsabili della corretta custodia del bene e durante l'utilizzazione dello stesso dovranno comportarsi in maniera diligente e responsabile, garantendo l'integrità materiale e del suo impiego.

In caso di danneggiamento, furto, smarrimento o utilizzo illecito, potranno essere attivate azioni di natura disciplinare e afferenti il risarcimento del danno come previsto dagli artt. 1218, 2043 e ss. cod. civ.

Si precisa inoltre che:

- il gestore telefonico fornisce i tabulati delle telefonate effettuate da ciascuna utenza dell'Istituto e che pertanto quest'ultimo potrà, in caso di necessità, effettuare controlli sul corretto utilizzo;
- i dati salvati sul dispositivo (rubrica, agenda) sono e restano di esclusiva responsabilità del singolo utente, che deve occuparsi di provvedere ai necessari backup o salvataggi;
- qualsiasi problema, disfunzione o rottura del dispositivo, va comunicata all'Istituto;
- in caso di interruzione del rapporto di lavoro tutti i dati istituzionali presenti nel dispositivo (es. rubrica telefonica) devono essere restituiti unitamente all'apparecchio.

Utilizzo dei computer

Ad ogni utilizzo di un PC o di computer fisso, l'addetto si assume la responsabilità del corretto utilizzo dello strumento nel rispetto delle istruzioni che seguono:

- le postazioni sono configurate secondo gli standard dell'Istituto e qualsiasi modifica deve essere autorizzata dall'Amministratore di Sistema, responsabile dei servizi informativi;
- è vietata l'istallazione sul computer di qualsiasi tipo di software senza l'autorizzazione della Dirigenza, al fine di prevenire l'istallazione di software pericolosi (quali ad esempio virus informatici che possono alterare la stabilità dei sistemi operativi) o sprovvisti di regolare licenza d'uso (d.lgs. 29 dicembre 1992, n. 518, L. 18 agosto 2000, n. 248);
- è vietato, se non a seguito di esplicito consenso o richiesta da parte dell'Istituto, collegare il computer ad altri computer, reti esterne, a modem, a router, a schede di rete o a qualsiasi dispositivo compreso telefono cellulare o periferica che non siano quelle previste dall'Istituto stesso;
- in presenza di terzi, è necessario accertarsi che questi non possano accedere alle informazioni contenute nel PC;
- è fatto divieto di caricare sul PC dati estranei all'attività lavorativa;
- una volta attivato il PC, è opportuno non lasciare incustodita la postazione senza prima averne bloccato l'accesso;
- l'utilizzo di eventuali supporti esterni da parte del personale amministrativo- oltre a dover essere autorizzato - deve essere preceduto da una opportuna verifica che accerti: l'origine del supporto, il suo contenuto e l'assenza di virus al suo interno;
- non è consentito utilizzare programmi informatici o strumenti per intercettare, falsificare, alterare o sopprimere, per finalità illecite, il contenuto di comunicazioni e/o documenti informatici.

L'Istituto si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere potenzialmente pericolosi per la sicurezza del sistema, ovvero acquisiti o istallati in violazione del presente regolamento.

3. Istruzioni per il corretto trattamento dati con strumenti informatici personali

Dotazioni degli strumenti

Qualora il dipendente utilizzi propri dispositivi, gli strumenti devono essere dotati almeno delle seguenti misure minime

- Software aggiornato
- Antivirus

- Accesso ad uno spazio cloud per effettuare il backup dei dati

Password

È obbligatorio l'uso corretto della propria password di accesso al PC, del cui utilizzo ogni incaricato è pienamente responsabile. È indispensabile che ciascun incaricato prenda nota delle buone modalità con cui è possibile selezionare parole chiave di difficile individuazione, seguendo le norme indicate di seguito. Qualora si abbia il sospetto che la propria password sia stata in qualche modo compromessa o venuta a conoscenza di terzi, si raccomanda di provvedere immediatamente alla sua sostituzione e riferire l'accaduto al responsabile d'Istituto.

Al fine di mantenere l'adeguata protezione della propria password:

- la parola chiave prescelta non deve mai contenere riferimenti personali (nomi, date di nascita, ecc., né dovrebbe rappresentare una parola in qualsiasi lingua o dialetto sufficientemente diffuso;
- si suggerisce di selezionare una nomenclatura della password adeguatamente lunga (minimo 8 caratteri) e complessa (caratteri maiuscoli, minuscoli, numeri e caratteri speciali);
- si raccomanda di non utilizzare la stessa password utilizzata in altri sistemi di autenticazione, interni o esterni all'Istituto, come ad esempio l'accesso al proprio conto corrente bancario e/o altre attività non legate all'attività istituzionale;
- non è permesso condividere o concedere l'uso della parola chiave prescelta con alcun soggetto, interno o esterno all' Istituto;
- nel momento in cui si sostituisce la propria password, la nuova selezionata dovrebbe essere diversa da quelle già utilizzate in precedenza.

Posta elettronica

La posta elettronica diretta all'esterno della rete informatica istituzionale può essere intercettata da estranei, ed è pertanto sconsigliato l'invio di documenti di lavoro riservati senza l'utilizzo di adeguate protezioni.

L'invio di documenti o dati mediante posta elettronica deve sempre essere effettuato con le dovute cautele, quali accertarsi che il destinatario sia autorizzato a trattare i dati inviati, che l'indirizzo sia corretto, che il destinatario riceva correttamente i documenti inviati (ad es. mediante conferma di lettura), ecc.

Per eventuali necessità, si suggerisce di apporre il seguente testo standard in calce:

"Qualora il messaggio fosse pervenuto per errore, preghiamo di cancellarlo immediatamente senza visionarne il contenuto e, se possibile, darcene gentilmente notizia. Il Titolare. non si assume alcuna responsabilità per eventuali intercettazioni, modifiche o danneggiamenti del presente messaggio email e/o eventuali allegati".

L'invio di documenti, contenenti dati particolari o particolarmente sensibili, per mezzo della posta elettronica, va effettuato previa protezione della documentazione con una password. Quest'ultima dovrà essere condivisa con il destinatario prima dell'invio o comunque con un mezzo separato rispetto all'email, nel cui corpo NON dovrà essere segnata in chiaro la password prescelta.

In generale, nell'utilizzo della posta elettronica come strumento di lavoro e di comunicazione tra i dipendenti, e tra questi e i terzi, si raccomanda in particolare di rispettare i criteri minimi di utilizzo riportati di seguito.

NON è consentito:

- dar luogo o rispondere a email "tipo catena di Sant'Antonio" dall'indirizzo istituzionale;
- inviare immagini, file, video o scherzi elettronici dall'indirizzo istituzionale;
- aprire allegati non sicuri, o inviati da fonti sconosciute;
- cancellare, anche parzialmente, le e-mail istituzionali inviate e/o ricevute, salvo diversa autorizzazione;
- cancellare, anche parzialmente, la rubrica istituzionale;
- cliccare su link.

È invece obbligatorio:

- eliminare tempestivamente messaggi "spam" o similari (onde evitare la diffusione di virus informatici).

Procedura d'emergenza

Qualora il Titolare necessiti di dover accedere al PC assegnato ad un dipendente ovvero alla Sua posta elettronica sarà onere del Responsabile dell'area o della Dirigenza stabilirne le modalità che potranno essere diversificate, area per area, nel rispetto delle regole che seguono:

- il responsabile dell'area, d'accordo con il dipendente, potrà individuare i colleghi autorizzati ad accedere alla sua casella di posta elettronica e/o alla propria postazione di lavoro in caso di assenza programmata;
- in caso di assenza non programmata, il dipendente potrà autorizzare anche telefonicamente il proprio responsabile o i propri colleghi ad accedere alla propria casella email e/o postazione di lavoro;
- in caso di necessità/urgenza/impossibilità a contattare il dipendente assente, l'Amministratore di Sistema, su richiesta della Dirigenza, potrà provvedere a resettare la password dell'utente, per consentirne l'accesso. Tale operazione verrà comunicata al dipendente non appena possibile. Al suo rientro, questi imposterà una nuova password;
- in ogni caso, è fatto divieto di "rispondere" utilizzando l'account email del dipendente assente;
- ogni utente ha l'obbligo di inserire un messaggio automatico di assenza;
- qualora la parola chiave venga utilizzata in assenza dell'incaricato, a quest'ultimo non compete più alcuna ulteriore responsabilità, in merito a trattamenti non autorizzati o accessi non consentiti ai dati. La sua responsabilità verrà pienamente rimessa in essere non appena avrà avuto la possibilità di selezionare una nuova parola chiave e assumere quindi la piena responsabilità del corretto utilizzo.

4. Istruzioni per il corretto trattamento dati con strumenti cartacei

Consegna dei documenti via posta

Nel caso la consegna di documenti, originali o fotocopiati contenenti dati particolari o informazioni qualificate come riservate, avvenga per posta tradizionale, si richiede l'utilizzo di tipi di spedizione che garantiscano di tracciare i movimenti del documento (ad es. raccomandata, etc.).

Quale che sia il tipo di spedizione adottato, si raccomanda di accertare che esso consenta di avere prova certa del fatto che il destinatario abbia effettivamente ricevuto i documenti inviati e che essi siano giunti integri, e quindi non manomessi o alterati in fase di trasporto.

Custodia dei documenti all'esterno dei luoghi di lavoro

Qualora per motivi di lavoro vengano trasportati documenti all'esterno del luogo di lavoro, l'incaricato deve tenere sempre sotto controllo il plico, avendo cura altresì che nessun soggetto terzo non autorizzato possa vedere anche solo la copertina del documento in questione.

5. Conversazioni e comunicazioni telefoniche

Si raccomanda di non discutere, comunicare o comunque trattare dati istituzionali se non si è certi che il corrispondente sia un incaricato autorizzato a trattare i dati in questione.

Si raccomanda la massima attenzione nella scelta dei luoghi ove svolgere le conversazioni telefoniche.

6. Social Network

La divulgazione di informazioni all'esterno, ad esempio attraverso i social networks, dovrà avvenire nel rispetto del principio di segretezza e riservatezza, nel rispetto del proprio profilo di autorizzazione e sempre salvaguardando l'immagine dell'Istituto.

C. DISCIPLINARE PER L'AUTORIZZATO AL TRATTAMENTO

Per i trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici, gli Autorizzati al trattamento dei dati personali debbono osservare le seguenti disposizioni.

Gli autorizzati al trattamento dei dati personali possono effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato nella nomina ricevuta con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati dell'Istituto che contengono i predetti dati personali.

II trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati.

L'Autorizzato al trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente

Ogni Autorizzato al trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

Gli Autorizzati al trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.

La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'Autorizzato.

L'Autorizzato del trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.

In caso di trattamento di dati sensibili e di dati giudiziari la componente riservata delle credenziali di autenticazione (parola chiave) deve essere modificata almeno ogni tre mesi.

Gli autorizzati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici gli autorizzati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'Autorizzato del trattamento non dovrà lasciarli mai incustoditi.
- L'Autorizzato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
- Al termine dell'orario di lavoro l'Autorizzato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Si deve adottare ogni cautela affinchè ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.
- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro Autorizzato debitamente autorizzato.
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
- Documenti contenenti dati personali che, per una qualunque ragione, siano da cestinare, devono assolutamente essere distrutti in modo da risultare illeggibili a soggetti terzi non autorizzati che ne potrebbero entrare in possesso (es. addetti alle pulizie).
- Quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'Autorizzato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.

L'Autorizzato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.

E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un autorizzato a potere trattare i dati in questione.

Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico o aperto al pubblico.

D. PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI – DATA BREACH

Il **GDPR** disciplina il **Data Breach**, ovvero le procedure che un'organizzazione pubblica o privata deve adottare in caso di incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

Si verifica un caso di data breach se si verifica una divulgazione o un accesso non autorizzato o accidentale, se si verifica un'alterazione o la perdita, l'impossibilità di accesso o la distruzione, accidentale o non autorizzata, di dati personali.

Ovviamente in questi casi non rientra solamente il furto o il danno provocato da soggetti terzi malintenzionati, ma **anche la perdita accidentale**, quindi la cancellazione di dati per un errore umano o di sistema, o semplicemente l'impossibilità di accesso al dato, per esempio la perdita della password di accesso ad un archivio protetto, o la criptazione provocata da un'infezione da ransomware.

L'autorità di controllo a cui segnalare il Data Breach è il **Garante della Privacy**, come definito dall'articolo 55 del General Data Protection Regulation.

Assenza di rischi

In caso non ci fosse alcun rischio connesso all'attacco verso i dati personali immagazzinati, è necessario registrare la violazione e successivamente conservare il registro. **La notifica al Garante della Privacy non è obbligatoria ed è comunque necessario comprovare l'assenza dei rischi.**

Presenza di rischi

In presenza di rischi per gli interessati è necessaria la **notifica entro 72 ore** al **Garante della Privacy**, il quale rilascia un apposito modulo (Modello di segnalazione Data Breach).

La procedura da seguire è:

1. Raccogliere tutte le informazioni inerenti al **Data Breach** per la notifica al **Garante della Privacy**
2. Inviare la notifica al **Garante della Privacy**
3. Registrare la violazione
4. Conservare il registro delle violazioni

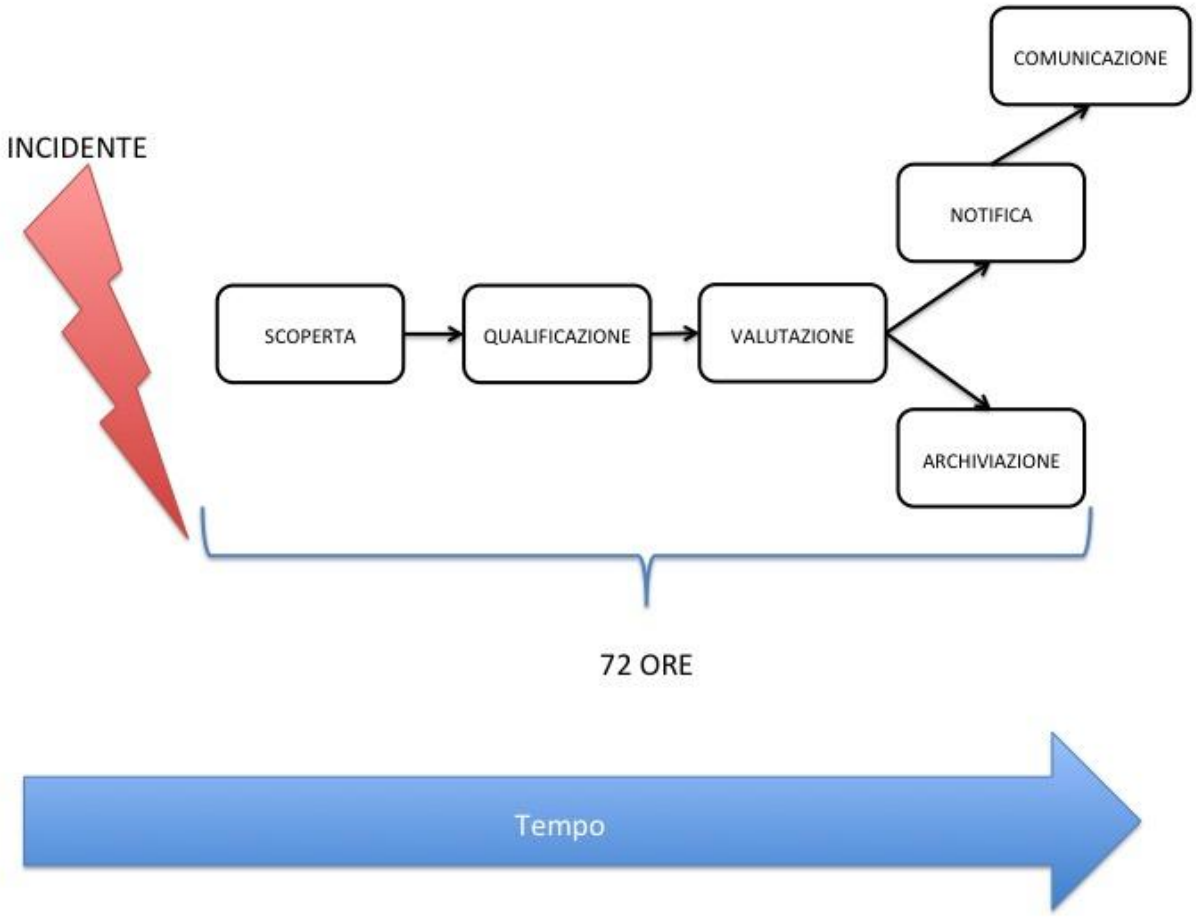
Presenza di un elevato rischio

La procedura da seguire è:

1. Raccogliere tutte le informazioni inerenti al **Data Breach** per la notifica al **Garante della Privacy** e ai diretti interessati del trattamento
2. Inviare la notifica al **Garante della Privacy** e **agli interessati**
3. Gestione dei riscontri da parte degli interessati
4. Registrare la violazione
5. Conservare il registro delle violazioni

Per un rischio elevato si intende per esempio una violazione che interessa un rilevante quantitativo di dati personali e/o di soggetti interessati, piuttosto che un **Data Breach** che impatta su soggetti vulnerabili per le loro condizioni o categorie particolari di dati personali.

Come notificare una violazione



Rilevazione del Data Breach

A. Canali interni

Le segnalazioni interne di eventi anomali possono:

- pervenire dal personale dell'Istituto;
- essere inoltrate dal DPO.

B. Canali esterni

Le segnalazioni possono pervenire anche da fonti esterne, o anche dall'analisi di informazioni presenti sul Web, ovvero dai Responsabili.

Inoltre, ogni Interessato può segnalare, anche solo in caso di sospetto, che i propri Dati Personali siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'Interessato può richiedere all'Istituto la verifica dell'eventuale violazione.

Per la segnalazione è necessario compilare la Scheda Evento, allegato alla presente procedura, contenente tutte le informazioni raccolte:

- Data evento anomalo;
- Data presunta di avvenuta violazione;
- Data e ora in cui si è avuto conoscenza della violazione;
- Fonte segnalazione;
- Tipologia di violazione e di informazioni coinvolte;
- Descrizione evento anomalo;
- Numero Interessati coinvolti;
- Numerosità di Dati Personali di cui si presume una violazione;
- Indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di Device Mobili;
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

La Scheda Evento viene consegnata al Titolare che può farsene carico o designare un delegato.

Le segnalazioni, a qualunque soggetto/funzione pervengano, devono essere tempestivamente comunicate al DPO comunque non oltre 12 ore dalla conoscenza della violazione, ove possibile a mezzo PEC.

La presa in carico di tutte le segnalazioni è di responsabilità del DSGA che provvederà a gestirle coinvolgendo le altre funzioni interessate secondo quanto specificato nella presente procedura.

La consapevolezza del titolare è considerato il momento in cui iniziano a decorrere i termini della notifica: è importante avere un "ragionevole grado di certezza" dato da indagini approfondite, quando necessarie.

Se l'incidente di sicurezza richiede maggiori controlli e verifiche, non è possibile ancora ritenere sufficiente la conoscenza dei fatti tanto da dover notificare l'accaduto.

Tuttavia sarà un'azione tempestiva, anche se solo di indagine, a rendere corretto il comportamento del titolare che quindi non dovrà prorogare troppo a lungo la fase investigativa.

Quando il titolare, anche quando ha appurato con ragionevole certezza l'esistenza di una violazione, non è già in possesso di tutti gli elementi utili per effettuare una descrizione completa ed esaustiva dell'infrazione, può adottare alcune tecniche o modalità che permettono di bilanciare le esigenze di celerità del messaggio con quelle di una sua sostanziale accuratezza e completezza.

Approssimazione: il titolare che non sia ancora in grado di conoscere con certezza il numero di persone e di dati personali interessati dalla violazione può comunicarne in prima battuta un ammontare approssimativo, provvedendo a specificare il numero esatto a seguito di accertamenti.

Notificazione in fasi: in questo caso il titolare, per la complessità o estensione della violazione, potrebbe non essere in grado di fornire con immediatezza all'autorità tutte le informazioni necessarie. Potrà allora ottemperare agli obblighi di

notifica comunicando, dopo una prima e rapida notifica di *alert*, tutte le informazioni per fasi successive, aggiornando di volta in volta l'autorità sui nuovi riscontri.

Notifica differita: dopo le 72 ore previste dall'art. 33. È il caso in cui, per esempio, un'impresa subisca violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al titolare e l'invio scaglionato di un numero elevato di notificazioni tra loro identiche, il titolare è autorizzato ad eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

Anche il responsabile del trattamento potrà notificare la violazione per conto del titolare, anche se a lui restano le responsabilità a essa collegate.

Analizzare la violazione e valutarne i rischi connessi

L'analisi consente al titolare di individuare con prontezza adeguate misure per arginare o eliminare l'intrusione e di valutare la necessità di attivare le procedure di comunicazione e di notifica (che si ricorda si attivano solo al superamento di determinate soglie di rischio).

Obiettivo dell'analisi di primo livello è quella di verificare che la segnalazione non si tratti di un cd. "falso positivo".

Nel caso la violazione su dati personali venga accertata il Titolare o il suo delegato recupera le informazioni di dettaglio sull'evento necessarie alle analisi di secondo livello, e le riporta nella Scheda Evento.

Nel caso in cui l'evento segnalato risulti essere un falso positivo, si chiude l'incidente e la funzione IT/Security si attiva per effettuare un raffinamento delle regole di rilevazione dei falsi positivi, comunicando via e-mail l'esito dell'analisi al Titolare.

L'evento viene comunque inserito a cura del Titolare o del suo delegato nel Registro dei Data Breach nella apposita sezione dedicata agli "eventi falsi positivi".

Per l'analisi di secondo livello vengono analizzate congiuntamente tutte le informazioni raccolte e redige una Scheda Violazione Dati per le conseguenti valutazioni.

L'evento viene classificato tra i seguenti casi:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
2. Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
3. Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

In particolari circostanze le violazioni potrebbero essere combinate tra loro.

La violazione deve essere valutata secondo i livelli di rischio:

- NULLO
- BASSO

- MEDIO
- ALTO

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'Interessato a cui si riferiscono i dati, a causa della violazione dei Dati Personali:

1. discriminazioni
2. furto o usurpazione d'identità
3. perdite finanziarie
4. pregiudizio alla reputazione
5. perdita di riservatezza dei dati personali protetti da segreto professionale
6. decifratura non autorizzata della pseudonimizzazione
7. danno economico o sociale significativo
8. privazione o limitazione di diritti o libertà
9. impedito controllo sui dati personali all'interessato
10. danni fisici, materiali o immateriali alle persone fisiche.

Saranno inoltre valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

a) che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;

b) che si tratti di dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;

c) che si tratti di dati di persone fisiche vulnerabili, in particolare minori;

d) che il trattamento riguardi una notevole quantità di Dati Personali;

e) che il trattamento riguardi un vasto numero di Interessati.

Il Titolare deve provvedere affinché vengano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della violazione.

Contenuto della notifica al Garante (Art. 33 p.3 GDPR)

La Comunicazione al Garante della violazione dei dati deve avere questi contenuti:

- Descrizione della 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.

- Il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.
- Descrizione delle probabili conseguenze della violazione dei dati personali.
- Descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Contenuto della Comunicazione agli interessati (Art. 34 p.3 GDPR)

In primo luogo il GDPR determina l'essenzialità della **notifica della violazione** dei dati all'autorità e della **comunicazione** ai soggetti interessati quando il data breach mette a rischio le **libertà** e i **diritti** di un individuo quali:

- Danni fisici, materiali o morali
- Danni economici o sociali
- Perdita del controllo dei dati
- Limitazione dei diritti
- Discriminazione
- Furto o usurpazione d'identità
- Perdite finanziarie
- Decifratura non autorizzata della pseudonimizzazione
- Pregiudizio alla reputazione
- Perdita di riservatezza dei dati protetti da segreto professionale (sanitari, giudiziari)

Mentre per far scattare l'obbligo di notifica è sufficiente che sussista una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, per la comunicazione occorre che tale rischio sia indicato come ALTO nella Scheda Violazione Dati.

La comunicazione all'interessato non è tuttavia richiesta se si ravvisano una serie di circostanze specifiche:

- quando il titolare del trattamento ha messo in atto, e applicato ai dati che sono stati oggetto di violazione, tutte le necessarie misure tecniche e organizzative di protezione, comprese quelle destinate a rendere i dati personali incomprensibili ai soggetti non autorizzati (come, ad esempio, la cifratura delle informazioni).
- quando il titolare del trattamento abbia successivamente adottato misure per scongiurare il verificarsi di un rischio elevato per i diritti e le libertà degli interessati.
- quando la comunicazione stessa richiederebbe sforzi sproporzionati e, in tal caso, si può procedere a una comunicazione pubblica o ad altra soluzione analoga, così da informare gli interessati in maniera ugualmente efficace.

In sostanza, dunque, è opportuno procedere a un duplice controllo: da un lato, occorre verificare che siano state adottate le misure di protezione adeguate, così da poter stabilire se c'è stata violazione dei dati personali e informare, di conseguenza, l'autorità di controllo e gli interessati. Dall'altro, si deve stabilire se la notifica è stata trasmessa senza ingiustificato ritardo, tenendo conto, in particolare, della natura e della gravità della violazione, nonché delle sue conseguenze ed effetti negativi per l'interessato.

Devono sempre essere **privilegiate modalità di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti).** Il messaggio dovrebbe essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di *update* generali o *newsletter*, che potrebbero essere facilmente fraintesi dai lettori. Inoltre, dovrebbe tenere conto di possibili formati alternativi di visualizzazione del messaggio e delle diversità linguistiche dei soggetti riceventi (es. l'utilizzo della lingua madre dei soggetti riceventi rende il messaggio immediatamente comprensibile).

Anche in questo caso, il Regolamento è attento a non gravare i titolari di oneri eccessivi prevedendo che, nel caso la segnalazione diretta richieda sforzi sproporzionati, questa possa essere effettuata attraverso una comunicazione pubblica. Si sottolinea però che anche questo tipo di comunicazione deve mantenere lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato. Così, mentre può ritenersi adeguata la comunicazione fornita attraverso evidenti *banner* o notifiche disposte sui siti web, non lo sarà se questa sia limitata all'inserimento della notizia in un blog o in una rassegna stampa.

La comunicazione agli interessati deve avere questi contenuti:

- Descrizione con un linguaggio semplice e chiaro della natura della violazione dei dati personali.
- Data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
- Il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.
- Descrizione delle probabili conseguenze della violazione dei dati personali.
- Descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Il registro dei data breach

L'art. 33 p.5 del GDPR, prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

Ne discende che le generali attività di scoperta dell'incidente, come le successive di trattamento, devono essere documentate, adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.

Il **registro dei data breach** è una documentazione che, ai sensi dell'art. 33 del GDPR, il titolare del trattamento è tenuto a conservare per tenere traccia di tutti i data breach avvenuti.

I titolari del trattamento sono tenuti a conservare un registro dei data breach che deve contenere le seguenti informazioni:

- i dettagli relativi al data breach, ovvero informazioni inerenti le cause della violazione, il luogo nel quale essa è avvenuta e la tipologia dei dati personali violati
- gli effetti e le conseguenze della violazione
- il piano di intervento predisposto dal titolare
- la motivazione delle decisioni assunte a seguito del data breach nei casi in cui:

- il titolare ha deciso di non procedere alla notifica
- il titolare ha ritardato nella procedura di notifica
- il titolare ha deciso di non notificare il data breach agli interessati

Il registro dei data breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

Il titolare del trattamento dovrà registrare nel registro il data breach che ha coinvolto la Struttura contestualmente alla comunicazione al Garante, avendo cura di inserire tempestivamente gli elementi che dovessero emergere all'esito di ulteriori verifiche.

Il registro dei data breach dovrà inoltre essere strutturato in modo da garantire l'integrità e l'immodificabilità delle registrazioni in esso contenute.

Ecco alcuni esempi commentati di violazione

Un supporto (cd/dvd/cassetta/ecc.) contenente un backup criptato con dati personali viene perso o rubato.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: No.

Commento: Se i dati vengono crittografati con un algoritmo di ultima generazione, esistono dei backup dei dati e la chiave privata non è compromessa, non è necessario notificare la violazione. Tuttavia, se venisse compromessa anche successivamente, la notifica diverrà necessaria.

Durante un cyber-attacco al sito web vengono rubati dati personali.

- Comunicazione al Garante: Sì, la notifica è necessaria in caso di potenziali danni ai soggetti interessati.
- Comunicazione agli interessati: Sì, la notifica dipende dalla natura dei dati violati e se è alto il livello di gravità dei potenziali danni.

Commento: Se il rischio non è elevato, consigliamo al titolare del trattamento di informare l'interessato, a seconda delle circostanze del caso. Ad esempio, la notifica potrebbe non essere necessaria in caso di violazione della riservatezza per una newsletter relativa ad un programma televisivo, mentre la notifica può essere richiesta se questa newsletter può portare a conoscenza del punto di vista politico del soggetto interessato.

Una breve interruzione dell'alimentazione del call center del titolare del trattamento, che comporta l'impossibilità dei clienti di chiamare il titolare del trattamento e di accedere ai propri dati.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: No.

Commento: Questa non è una violazione dei dati personali da notificare, ma solo un incidente di cui tenere nota ai sensi dell'art. 33, paragrafo 5.
Il titolare del trattamento dovrà redigere un apposito registro.

Un titolare del trattamento subisce un attacco ransomware che causa la crittografia di tutti i dati. Nessun back-up è disponibile e i dati non possono essere ripristinati. Al momento dell'indagine, risulta evidente che l'unico scopo del ransomware era quello di crittografare i dati e che nessun altro malware veniva rilevato nel sistema.

- Comunicazione al Garante: Sì, la notifica è necessaria in caso di potenziali danni ai soggetti interessati, visto che questo attacco comporta una perdita di disponibilità dei dati.
- Comunicazione agli interessati: Sì, la notifica dipende dalla natura dei dati violati e dal possibile effetto della perdita di disponibilità dei dati, così come altre probabili conseguenze.

Commento: Se fosse disponibile un backup e se i dati potessero essere ripristinati in tempo utile, non sarebbe necessario segnalare al Garante o agli interessati poiché non ci sarebbe stata perdita permanente di disponibilità o riservatezza. Tuttavia, il Garante potrebbe considerare di verificare la conformità dei requisiti di sicurezza più ampi previsti dall'art. 32.

Un interessato denuncia all'Istituto una violazione di dati. Il soggetto ha ricevuto un documento contenente dati di qualcun altro.

Il titolare del trattamento intraprende una breve indagine (che va completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e se ciò è stato causato da un difetto sistemico che comporti il potenziale interessamento di altri soggetti.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: Vengono notificati i soggetti interessati solo se esiste un rischio elevato ed è chiaro che altri soggetti non sono stati coinvolti.

Commento: Se, dopo ulteriori indagini, si è stabilito che sono interessati più soggetti, sarà necessario aggiornare il Garante ed il titolare del trattamento dovrà intraprendere, come azione supplementare, la notifica ad altri soggetti, in caso di loro rischio elevato.

Una società di hosting web individua un errore nel codice che controlla l'accesso da parte degli utenti. L'anomalia comporta che qualunque utente possa accedere ai dettagli dell'account di qualsiasi altro utente.

- Comunicazione al Garante: Come responsabile del trattamento, la società di hosting web deve notificare tempestivamente al Garante quali suoi clienti (titolari del trattamento) sono coinvolti. Supponendo che la società di hosting web abbia effettuato una propria indagine, i titolari coinvolti dovrebbero essere ragionevolmente sicuri di sapere o meno di aver subito una violazione. Pertanto è da considerarsi "avvisato" una volta che è stato oggetto di notifica dalla società di hosting (il responsabile del trattamento). Il titolare dovrà in seguito notificare la violazione all'autorità di vigilanza.
- Comunicazione agli interessati: Se non esiste un rischio elevato per i soggetti interessati, la notifica non è necessaria.

Commento: La società di hosting web (responsabile) deve considerare tutti gli altri obblighi di notifica (ad esempio, nell'ambito della direttiva NIS).

Se non vi è alcuna prova che questa vulnerabilità sia stata sfruttata da un particolare soggetto titolare, una notifica di violazione non può aver luogo ma è probabile che sia registrabile o che rientri nei casi di non conformità, ai sensi dell'art. 32.

Un attacco informatico causa la non disponibilità dei registri medici in un ospedale per il periodo di 30 ore.

- Comunicazione al Garante: Sì, l'ospedale è tenuto a notificare al paziente che potrebbe verificarsi un alto rischio per il suo benessere e la sua privacy.
- Comunicazione agli interessati: Sì, la notifica è necessaria.

I dati personali di 5000 studenti sono inviati per errore ad una mailing list sbagliata con più di 1000 destinatari.

- Comunicazione al Garante: Sì, la notifica è necessaria.
- Comunicazione agli interessati: Sì, la notifica è necessaria ai soggetti interessati, a seconda dell'ambito e tipo dei dati personali coinvolti e della gravità delle possibili conseguenze.

Una e-mail di marketing diretto viene inviata ai destinatari nel campo "a:" o "cc:", consentendo così a ciascun destinatario di visualizzare l'indirizzo di posta elettronica di altri destinatari.

- Comunicazione al Garante: Sì, la notifica all'autorità di vigilanza può essere obbligatoria se è coinvolto un numero elevato di soggetti, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, la mail contiene le password iniziali).
- Comunicazione agli interessati: Sì, la notifica è necessaria ai soggetti interessati, a seconda del tipo dei dati personali coinvolti e della gravità delle possibili conseguenze.

Commento: La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili o se viene rivelato solo un numero ristretto di indirizzi di posta elettronica.

SCHEDA EVENTO

CODICE	
Data evento e ora della violazione anche solo presunta (specificando se è presunta);	
Data e ora in cui si è avuto conoscenza della violazione;	
Fonte di segnalazione	
Tipologia evento anomalo	
Descrizione evento anomalo	
Numero interessati coinvolti	
Numerosità dei dati personali di cui si presume la violazione	
Data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza	
Luogo in cui è avvenuta la violazione dei dati (specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

SCHEDA VIOLAZIONE DATI

CODICE EVENTO[1]	CLASSIFICAZIONE[2]	RISCHIO[3]

[1] Inserire il CODICE della scheda evento

[2] L'Evento viene classificato tra i seguenti casi:

- distruzione di dati illecita,
- perdita di dati illecita,
- modifica di dati illecita,
- distruzione di dati accidentale,
- perdita di dati accidentale,
- modifica di dati accidentale,
- divulgazione non autorizzata
- accesso ai dati personali illecito.

[3] Il rischio deve essere valutato secondo i seguenti livelli di rischio:

- NULLO
- BASSO
- MEDIO
- ALTO

il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'interessato a cui si riferiscono i dati, a causa della violazione dei dati personali:

- discriminazioni
- furto o usurpazione d'identità
- perdite finanziarie
- pregiudizio alla reputazione
- perdita di riservatezza dei dati personali protetti da segreto professionale
- decifratura non autorizzata della pseudonimizzazione
- danno economico o sociale significativo
- privazione o limitazione di diritti o libertà
- impedito controllo sui dati personali all'interessato
- danni fisici, materiali o immateriali alle persone fisiche.

REGISTRO DEI DATA BREACH

Evento				Conseguenze	Provvedimenti adottati	Notifica all'autorità di controllo		Comunicazione all'interessato	
Codice[4]	Falso Positivo	Irrilevante	Rilevante			SI/NO	Data	SI/NO	Data

[4] Inserire codice scheda evento

MODELLO DI COMUNICAZIONE AGLI INTERESSATI DELLA VIOLAZIONE DEI DATI

G.mo Utente,

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) 679/2016, L'Istituto _____, titolare del trattamento, con la presente è a comunicarLe, l'intervenuta violazione dei Suoi dati personali (data breach) che si è verificata in data _____[5], alle ore_____;[6]

NATURA DELLA VIOLAZIONE

_____

_____

_____

TIPO DI VIOLAZIONE:

☐ Lettura (presumibilmente i dati non sono stati copiati)

☐ Copia (i dati sono ancora presenti sui sistemi del titolare)

☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

☐ _____

DISPOSITIVO OGGETTO DI VIOLAZIONE:

☐ Computer,

☐ Rete,

☐ Dispositivo mobile

[5] A. Tra il __e il____
B. In un tempo non ancora determinato
C. È possibile che sia ancora in corso

[6] Indicare l'ora se nota, altrimenti indicare l'ora in cui si viene a conoscenza della violazione.

- ☐ Strumento di backup
- ☐ Documento cartaceo
- ☐ _____

CHE TIPO DI DATI SONO OGGETTO DI VIOLAZIONE PER ESEMPIO:

- ☐ Dati anagrafici (nome, cognome, numero di telefono, e mail, CF, indirizzo ecc..)
- ☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica
- ☐ Dati personali idonei a rivelare le convinzioni religiose
- ☐ Dati personali idonei a rivelare filosofiche o di altro genere
- ☐ Dati personali idonei a rivelare le opinioni politiche
- ☐ Dati personali idonei a rivelare l'adesione a partiti
- ☐ Dati personali idonei a rivelare sindacati,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere religioso,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere filosofico,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere politico
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute
- ☐ Dati personali idonei a rivelare la vita sessuale
- ☐ Dati giudiziari
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ _____

NOME E DATI DI CONTATTO DEL DPO O UN ALTRO PUNTO DI CONTATTO PRESSO CUI OTTENERE PIÙ INFORMAZIONI:

_____

DESCRIZIONE DELLE PROBABILI CONSEGUENZE DELLA VIOLAZIONE

_____

_____

DESCRIZIONE DELLE MISURE ADOTTATE O DI CUI SI PROPONE L'ADOZIONE PER PORRE RIMEDIO ALLA VIOLAZIONE DEI DATI PERSONALI[7]

_____

_____

Scusandoci per quanto avvenuto rimaniamo a Sua disposizione per eventuali chiarimenti.

Firma Istituto

[7] e anche, se del caso, per attenuarne i possibili effetti negativi