DISPOSIZIONI DI ENGIM IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

CONFORMI AL GDPR 679/16 E AL D.LGS 196/2003

Versione: 00

Data emissione: 25/05/2018

SOMMARIO

1. DOCUMENT MANAGEMENT

Dati Organizzazione

Ragione Sociale:	Engim LOMBARDIA
Forma Giuridica:	Associazione riconosciuta
Attività:	Istruzione e Formazione
P.IVA e C.F.:	03485690162
Nazione:	Italia
Provincia:	BG
Comune:	Valbrembo
Indirizzo:	Via Sombreno,2
CAP:	24030
Telefono:	035527853
Email:	info@engimlombardia.org
Sito Internet:	www.lombardia.engim.org

Dati Sistema Privacy

Nome Sistema Privacy:	Sistema Privacy
Obiettivo Politica:	Il presente documento comprende tutti gli elementi che compongono il sistema per la protezione dei dati ai sensi del Regolamento Europeo 679/2016 (GDPR). Il presente documento è redatto dal Titolale del trattamento e sarà aggiornato ogni qual volta verrà applicata una variazione al sistema privacy in precedenza implementato.
Norme di Riferimento:	Regolamento Europeo 679/2016 , D.Lgs 196/03
Interlocutori per la redazione del documento	Direttore

2. INTRODUZIONE

Il presente Regolamento sulla protezione dei dati personali (di seguito "Regolamento") di ENGIM LOMBARDIA, Titolare del trattamento dei dati (infra anche "Istituto"), è redatto e aggiornato in conformità al ***Regolamento (UE) n. 679/2016 in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali e di libera circolazione di tali dati*** (di seguito "Reg. 679/2016") nonché al D.lgs 196/03.

Il presente documento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali, con le pronunce del Garante della Privacy e con le linee guida del Working Party ex Articolo 29 Reg. UE.

L' Istituto sostiene e promuove, al suo interno, ogni strumento di applicazione che possa consolidare il pieno rispetto del diritto inviolabile alla riservatezza e migliorare la qualità del servizio di protezione dei dati personali degli interessati.
A tal riguardo, uno degli strumenti essenziali di sensibilizzazione è l'attività di formazione del personale e l'attività informativa diretta a tutti coloro che hanno rapporti con la Istituto.

Per garantire la conoscenza capillare delle disposizioni del Regolamento e del presente documento, è data a ogni dipendente una specifica comunicazione con i riferimenti per l'acquisizione del presente regolamento, pubblicato sul sito aziendale, contenente tutti i principi fondamentali in tema privacy, esposti in maniera semplice, chiara e puntuale.

Le prescrizioni descritte nel presente Regolamento si applicano a tutti i trattamenti eseguiti nell'ambito dell'intera struttura organizzativa dell' Istituto dai Responsabili e dagli Incaricati (come infra definiti), e sono da considerare vincolanti nei rapporti contrattuali relativi a trattamenti eseguiti da altri soggetti esterni cui sia conferito un incarico di Responsabile del trattamento di dati di cui la medesima Istituto sia Titolare.

Il presente documento riepiloga l'assolvimento degli adempimenti previsti sulla base della situazione organizzativa dell'istituto e del *privacy risk assessment*, descrivendo *ex multis* le misure di sicurezza adottate nel trattamento dei dati.
Tale documento ha anche lo scopo di definire, sulla base della predetta analisi dei rischi, i criteri e le procedure per garantire la sicurezza nel trattamento dei dati personali, la distribuzione dei

compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi, e in particolare:

a. i criteri a cui i dipendenti e i collaboratori devono attenersi nell'ambito della trattazione dei dati;
b. i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
c. i criteri e le procedure per assicurare l'integrità e la disponibilità dei dati;
d. i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;
e. i criteri e le procedure per il ripristino dell'accesso ai dati;
f. l'elaborazione di un piano di formazione per rendere edotti il personale interno del trattamento dei rischi individuati e delle modalità volte alla prevenzione di eventuali danni;
g. le modalità e le tempistiche di monitoraggio e di revisione periodica dell'efficacia delle predette procedure e criteri.

2.1. RIFERIMENTI NORMATIVI

- Fonti normative italiane
  - ✓ D.lgs. n. 196/03 - "Codice in materia di protezione dei dati personali";
  - ✓ Provvedimento del Garante per la protezione dei dati personali dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008;
  - ✓ Provvedimento del Garante per la protezione dei dati personali dal titolo "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" del 13 ottobre 2008, in G.U. n. 287 del 9 dicembre 2008;
  - ✓ Provvedimento in materia di Videosorveglianza dell'8 aprile 2010;
  - ✓ D.L. n. 70 del 13 maggio 2011;
  - ✓ Decreto Legge n. 201/2011;
  - ✓ Decreto Legge 9 febbraio 2012, n. 5;
  - ✓ ISO 27001:2013 "Sistemi di Gestione della sicurezza delle informazioni";

- ✓ D.lgs. 14 settembre 2015 n. 151: Riforma dell'art.4 dello statuto dei lavoratori;
- ✓ Direttiva (UE) n. 680/2016 che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini;

➢ Fonti normative comunitarie e internazionali

- ✓ Carta dei diritti fondamentali dell'Unione Europea;
- ✓ Trattato di Lisbona;
- ✓ Direttiva 2009/136 (*c.d. Direttiva e-privacy*) relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e s.m.i.;
- ✓ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (*c.d. Direttiva madre*);
- ✓ Linee guida del Gruppo di lavoro ex articolo 29.

3. CODICE DI CONDOTTA

Gentili Dipendenti e Collaboratori,

il rispetto delle normative giuridiche sulla protezione dei dati personali rappresenta un aspetto molto importante sia per poter offrire un'adeguata offerta formativa ai nostri clienti e dei nostri studenti, sia per impostare in modo efficace i nostri processi interni. Le moderne tecnologie di informazione e comunicazione rappresentano una parte integrante e fondamentale dei processi aziendali. Un utilizzo inadeguato e improprio di queste tecnologie può comportare una lesione dei diritti personali alla privacy.

Pertanto il nostro Istituto ha il dovere di mettere in primo piano la tutela dei diritti personali e soddisfare un livello adeguato di protezione, rilevamento e trattamento di dati dei clienti, degli studenti e della loro famiglie, dei partner contrattuali nonché dei dipendenti.

Consapevoli dell'importanza di questo obiettivo, l' Istituto e il suo personale si impegna ad attenersi al seguente Codice di Condotta.

3.1. OBIETTIVO DEL CODICE DI CONDOTTA

L'obiettivo del presente Codice consiste nello stabilire standard di protezione e sicurezza uniformi, adeguati e globali nell'interesse di ENGIM LOMBARDIA allo scopo di soddisfare i requisiti fissati dal *D.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali), della Direttiva (UE) n. 680/2016 e s.m.i. che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini e del Regolamento (UE) n. 679/2016 e s.m.i. in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali e di libera circolazione di tali dat*i (di seguito "Reg. n. 679/2016"). Il Codice di Condotta crea un livello di protezione dei dati uniforme in tutta la Istituto, coadiuvato da un contestuale supporto documentale che consolida l'attività di informativa sulla protezione dei dati personali, nonché la predisposizione di nomine dei soggetti coinvolti nel trattamento dei dati personali.

3.2. LIMITI DI VALIDITÀ

Il Codice di Condotta è valido sia per il trattamento dei dati personali dei clienti, alunni e famiglie sia per il trattamento dei dati dei fornitori, consulenti, collaboratori ed altri partner contrattuali che si interfacciano con la nostra realtà.

L'ammissibilità della raccolta e delle finalità del trattamento dei dati deve essere valutata sulla base delle norme nazionali, comunitarie e internazionali in materia privacy.

3.3. PRINCIPI AI QUALI ATTENERSI PER L'ELABORAZIONE DEI DATI PERSONALI

1. Nel trattamento dei dati è necessario tutelare i diritti personali alla privacy degli interessati.
2. I dati personali possono essere trattati esclusivamente se ciò risulta legalmente ammissibile o se il soggetto interessato ha fornito il proprio consenso. I dati personali possono essere elaborati esclusivamente ai fini per i quali sono stati originariamente raccolti.
3. I dati personali devono essere memorizzati correttamente e, qualora necessario, periodicamente aggiornati. A tale scopo occorre adottare provvedimenti idonei per cancellare o rettificare i dati che risultano incorretti o incompleti.

4. Ai dati personali possono accedere solo i dipendenti o i collaboratori che operano in un settore di attività connesso a trattamento di tali dati; l'autorizzazione all'accesso deve essere limitata in base al tipo e alla portata della rispettiva area di competenza.
5. I dati personali che non risultano più necessari ai fini commerciali per i quali sono stati originariamente raccolti e memorizzati, possono essere eventualmente cancellati in conformità con le norme vigenti sulla conservazione dei dati.
6. Qualora l'interessato si sia opposto all'utilizzo dei propri dati personali a scopo di marketing e/o profilazione, i dati non potranno essere utilizzati a tal fine.
7. Il trattamento dei dati deve essere finalizzato allo scopo di ottenere la minima quantità possibile di informazioni. Le possibilità di anonimizzazione e pseudonimizzazione sono ammesse, laddove ciò sia possibile e gli oneri di queste procedure risultino adeguatamente rapportati alle finalità di protezione dei dati che si intende perseguire.
8. Nei processi di trattamento dei dati dai quali possono derivare particolari rischi per la tutela del diritto alla privacy degli interessati, il settore Protezione Dati deve essere interpellato a partire dalle prime fasi del processo di trattamento.

3.4. TIPOLOGIE PARTICOLARI DI DATI PERSONALI

Il trattamento dei dati personali relativi alla provenienza razziale ed etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, all'appartenenza a sindacati oppure sulla salute o sull'orientamento sessuale dell'interessato è generalmente vietata, salvo che la legittimità dell'elaborazione non derivi da un'autorizzazione legale o da un requisito di legge.
In tutti gli altri casi, l'interessato deve avere fornito espressamente il proprio consenso al trattamento dei suddetti dati.

3.5. INFORMAZIONE E CONSENSO DELL'INTERESSATO

Il titolare del trattamento, al momento della raccolta dei dati personali, è tenuto a fornire all'interessato, avvalendosi del personale incaricato, l'informativa prevista dall'a*rt 13-14 del Reg. n. 679/2016*.

L'informativa è fornita per iscritto mediante appositi strumenti:

a. attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;
b. avvisi agevolmente visibili dal pubblico, posti nelle bacheche dell'istituto o sul sito dell'Istituto;
c. apposita avvertenza inserita nei contratti o nelle lettere di affidamento al servizio del personale dipendente, del personale convenzionato, dei fornitori di beni o di servizi, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionisti, ecc.

L'informativa deve contenere:

a. l'indicazione dei soggetti Titolari, Responsabili e incaricati del trattamento;
b. le finalità e le modalità del trattamento;
c. la base giuridica del trattamento;
d. l'indicazione della natura facoltativa del conferimento dei dati e le conseguenze dell'eventuale rifiuto al conferimento dati;
e. il trattamento dei dati in casi particolari;
f. l'indicazione dei diritti dell'utente;
g. l'ambito di comunicazione e diffusione dei dati;
h. ogni altra informazione prevista dall'art. 7 del reg. UE 679/16.

- ✓ Rapporto contrattuale: i dati personali dell'interessato possono essere rilevati ed elaborati sulla base e ai fini di esecuzione del contratto e dell'avviamento del rapporto di lavoro. In questo contesto è consentito anche l'utilizzo a fine di marketing, o di ricerche di mercato e sondaggi di opinione, nella misura in cui ciò risulti in accordo con lo scopo per i quali i dati sono stati originariamente rilevati. L'interessato deve essere consapevole od informato dell'identità del responsabile del trattamento, delle finalità del trattamento dei dati, dei terzi o categorie di terzi ai quali i dati possono essere eventualmente trasmessi e della possibilità di partecipare volontariamente ad azioni di marketing o ricerche di mercato e sondaggi di opinione.

  L'interessato deve essere informato dei Suoi diritti.
- ✓ Rapporto non contrattuale: qualora non sussista un rapporto contrattuale, l'interessato deve avere acconsentito al trattamento dei propri dati personali.

Prima di rilasciare il consenso, l'interessato deve essere informato.

La dichiarazione di consenso deve essere regolarmente rilasciata per iscritto. Qualora si tratti, ad esempio, di un consenso che viene rilasciato nell'ambito della conclusione di un contratto di compravendita, la clausola contrattuale che contiene il consenso deve essere evidenziata visivamente sul modulo del contratto di acquisto. Nella dichiarazione di consenso devono essere specificate le modalità e le finalità del trattamento dei dati.

- ✓ Scambio di dati con terzi/acquisizione di dati: qualora i dati vengano raccolti presso terzi o trasmessi da terzi, è necessario verificare che alla prima richiesta dei dati l'interessato sia stato o venga conformemente informato del presente Codice di Condotta.
- ✓ Scambio di dati all'interno del Gruppo (qualora presente): qualora una istituto del Gruppo giuridicamente autonoma trasmetta dati personali ad un'altra istituto del Gruppo, si tratta comunque di un trasferimento a terzi, e pertanto si richiedono le opportune cautele.

3.6. CONSENSO AL TRATTAMENTO DEI DATI

Il consenso è definito come "*qualsiasi manifestazione di volontà libera, specifica e informata, con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento*".

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento, con la stessa facilità con cui è accordato. La revoca de consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

3.7. DIRITTI DEGLI INTERESSATI

L'interessato è il soggetto, persona fisica, alla quale si riferiscono i dati oggetto del trattamento.

La Istituto attua tutte le misure necessarie a facilitare l'esercizio dei diritti dell'interessato ai sensi dell'*art. 7 del Codice della privacy e degli artt. 12-22 del Reg. n. 679/2016*.

L'interessato ha il diritto di ottenere dal Titolare del trattamento:

a. conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e di ottenere l'accesso ai dati personali con riguardo alle seguenti informazioni:
    - origine dei dati;
    - finalità e modalità del trattamento:

- la logica applicata e i criteri utilizzati nell'elaborazione elettronica dei dati;
- gli estremi identificativi del Titolare e del Responsabile del trattamento;
- i soggetti e le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza;
- periodo di conservazione dei dati personali e i criteri utilizzati per la determinazione di tale periodo.

b. ottenere una **comunicazione** dei dati, oggetto del trattamento, che sia concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate ai minori;
c. richiedere la **rettifica/aggiornamento** dei dati personali inesatti che lo riguardano; l'interessato ha diritto di ottenere l'**integrazione** dei dati personali incompleti, anche fornendo una dichiarazione integrativa;
d. ottenere la **cancellazione (diritto all'oblio)** dei dati personali che lo riguardano qualora sussista una delle ipotesi tassativamente previste dall'*art. 17, par. 1, lett. a) - f), Reg. n. 679/2016, salvo quanto previsto dall'art. 17, par. 2 Reg. n. 679/2016;*
e. ottenere la **trasformazione in forma anonima o il blocco** se trattati in violazione di legge;
f. ottenere la **limitazione del trattamento** dei dati qualora sussista una delle ipotesi tassativamente previste dall'*art. 18, par. 1, lett. a) - d), Reg. n. 679/2016*, affinché i dati personali siano trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro;
g. **ricevere** in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento (**diritto alla portabilità dei dati**) senza impedimenti da parte del titolare del trattamento cui li ha forniti, purché ciò non leda i diritti e le libertà altrui;
h. **proporre opposizione** in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano da parte dei quali si dovranno pertanto astenere dal successivo trattamento salvi i casi tassativamente previsti dalla legge;

i. **revocare il consenso** al trattamento dei dati in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, qualora il trattamento sia basato sul disposto dell'*art. 6, par. 1, lett. a), o dell'art. 9, par. 2, lett. a) Reg. n. 679/2016;*

j. **proporre reclamo** a un'autorità di controllo;

k. avere **informazione circa la fonte** da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico, qualora i dati non siano stati ottenuti presso l'interessato ai sensi dell'*art. 14 Reg. n. 679/2016*.

3.8. SISTEMI INFORMATICI DI SICUREZZA DEI DATI

I server, i personal computers, i tablet, gli smartphone, e ogni altro strumento informatico di proprietà di ENGIM LOMBARDIA e in possesso dei dipendenti e collaboratori, costituiscono il "Sistema Informatico Aziendale" (di seguito "SIA"; ciascuno strumento informatico di seguito "Strumento Elettronico").

Gli utenti del SIA devono servirsi degli strumenti informatici con diligenza, preservandone l'integrità ed il funzionamento.

Gli "Strumenti" e i relativi programmi e/o applicazioni affidati al dipendente sono strumenti di lavoro e pertanto:

- possono essere utilizzati solo per fini professionali ed aziendali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali, tantomeno per scopi illeciti;
- vanno custoditi in modo appropriato, ponendo particolare attenzione anche alla loro sicurezza fisica sia all'interno della istituto (lasciandoli in ufficio chiuso a chiave, dove possibile, o riposti in cassetti o armadi dotati di serratura) che all'esterno (ad esempio evitando di lasciarli incustoditi in autovettura o sui mezzi pubblici);
- il loro furto, danneggiamento o smarrimento deve essere prontamente segnalato a ENGIM LOMBARDIA;

Ai fini sopra esposti sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni.

Sarà cura della istituto adottare idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento del SIA, in tempi certi compatibili con i diritti degli interessati e non superiori a 72 ore.

3.9. PROVVEDIMENTI, SANZIONI E REPSONSABILITÀ

L' Istituto, in qualità di Titolare del trattamento dei dati, ha l'obbligo di garantire nei confronti degli interessati il rispetto dei requisiti di protezione dei dati personali, predisponendo, laddove sia necessario anche dei corsi di formazione.

I Responsabili e gli incaricati del trattamento devono essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste sanzioni amministrative pecuniarie e penali per eventuale uso non corretto dei dati oggetto di tutela.

In merito alla responsabilità civile l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

4. FUNZIONI ORGANIZZATIVE RELATIVE ALLA PRIVACY E ALLA PROTEZIONE DEI DATI PERSONALI

4.1. TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento (*data controller*) è il centro di imputazione giuridica del trattamento dei dati personali che, nella figura del legale rappresentante e avvalendosi dei Responsabili interni per il trattamento e, ove necessario, dei consulenti esterni, pone in essere le seguenti attività:

a. individua e prende decisioni in ordine alle finalità ed alle modalità di trattamento dei dati personali, ivi compreso il profilo della sicurezza –
b. adotta le idonee misure volte ad agevolare l'accesso ai dati personali da parte dell'interessato nonché a semplificare le modalità e a ridurre i tempi per il riscontro ai quesiti posti dall'interessato;
c. effettua il censimento ed aggiorna l'elenco dei trattamenti dei dati personali in azienda e garantisce il diritto d'accesso come previsto dalle norme sulla privacy;
d. nomina con proprio atto i Responsabili interni del trattamento dei dati personali, impartendo ad essi i compiti e le 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, all'adozione di misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
e. nomina un Data Protection Officer (nei casi previsti dalla legge)
f. nomina i responsabili esterni al trattamento dei dati personali ex art. 28 GDPR 679/16;
g. individua, predispone, verifica, documenta e rende note le misure tecniche e organizzative adeguate per garantire la protezione dei dati personali in conformità alla normativa vigente, considerati la natura, l'ambito di applicazione, l'oggetto, il contesto e le finalità del trattamento;
h. dispone verifiche periodiche per riesaminare e aggiornare le istruzioni impartite e le predette misure di sicurezza ogni qualvolta lo ritenga necessario;
i. redige, aggiorna e conserva le disposizioni aziendali in tema di Privacy.

4.2 RESPONSABILE INTERNO DEL TRATTAMENTO DEI DATI PERSONALI

Gli incaricati del trattamento sono le persone fisiche designate dal titolare del trattamento, incaricate di svolgere le operazioni di trattamento dei dati personali di sua competenza con l'indicazione puntuale dei compiti, dell'ambito di trattamento consentito e delle modalità cui deve attenersi per l'espletamento dell'incarico.

Ciascun dipendente è assegnato, al momento dell'assunzione o nel caso di cambiamento di mansione, presso un'unità organizzativa ove sono trattati i dati e per ciascuna delle quali sono individuate le categorie di dati cui si può avere accesso e gli ambiti del trattamento.

La nomina è effettuata per iscritto con l'indicazione di idonee e analitiche istruzioni per operare con la massima diligenza e attenzione e rispettando le misure di sicurezza predisposte dalla Istituto.

L'incaricato collabora con il Titolare segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per lo svolgimento di una corretta attività di controllo di questi ultimi.

L'incaricato del trattamento deve assicurare che i dati siano:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b. raccolti per le finalità determinate, esplicite e legittime individuate dal Titolare e dal Responsabile del trattamento;
c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità;
d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti;
e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali i dati sono stati acquisiti;
f. trattati in modo tale che venga ad essa garantita un'adeguata sicurezza dei dati personali.

4.3. RESPONSABILI ESTERNI DEL TRATTAMENTO DEI DATI PERSONALI

Tutti i soggetti che effettuano operazioni di trattamento dei dati forniti dalla Istituto, per conto e nell'interesse di ENGIM LOMBARDIA, per finalità connesse all'esercizio dell'attività aziendale, sono considerati **Responsabili esterni del trattamento**, in virtù di specifico contratto (lettera di nomina) sottoscritto dalle parti.

I Responsabili esterni del trattamento hanno l'obbligo di:

a. trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia di privacy;
b. rispettare le misure di sicurezza di cui all'*art. 32 del Reg. n. 679/2016*;
c. nominare al loro interno gli incaricati del trattamento;
d. trattare i dati personali in conformità alle istruzioni e per le finalità previste nel contratto;
e. attenersi alle disposizioni impartite dal Titolare del trattamento;
f. specificare i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti.

Nel caso di mancato rispetto delle predette disposizioni e in caso di mancata comunicazione dell'atto di nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso la Istituto, il Responsabile esterno del trattamento.

I responsabili esterni dovranno far pervenire senza ritardo al Titolare del trattamento idonea documentazione con riferimento agli accordi stipulati che comportano il trattamento dei dati all'esterno della Istituto, unitamente all'atto di nomina a Responsabile esterno del trattamento controfirmato per accettazione.

4.3. IL CLOUD COMPUTING

Con il termine *cloud computing*, o semplicemente cloud, ci si riferisce a un insieme di tecnologie e di modalità di fruizione di servizi informatici che favoriscono l'utilizzo e l'erogazione di software, la possibilità di conservare e di elaborare grandi quantità di informazioni via Internet.

Il cloud offre, a seconda dei casi, servizi di conservazione o di elaborazione dei dati dai computer degli utenti ai sistemi del fornitore.

Il cloud consente, inoltre, di usufruire di servizi complessi senza doversi necessariamente dotare né di computer e altri hardware avanzati, né di personale in grado di programmare o gestire il sistema.

Con riferimento all'architettura del cloud, si distinguono:

a. Private cloud (PRC): infrastruttura informatica per lo più dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo.
b. Public cloud (PUC): l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o amministrazioni i propri sistemi attraverso la condivisione e l'erogazione via Internet di applicazioni informatiche, di capacità elaborativa e di "stoccaggio" dati.
c. Hybrid cloud (HYC): soluzioni che prevedono l'utilizzo di servizi erogati da infrastrutture private accanto a servizi acquisiti da cloud pubblici.
d. Community cloud (COC): l'infrastruttura è condivisa da diverse organizzazioni a beneficio di una specifica comunità di utenti.

L' Istituto deve prestare particolare attenzione ai rischi connessi all'adozione dei servizi di cloud computing, anche in relazione agli aspetti di protezione dei dati personali.

L' Istituto, in qualità di Titolare del trattamento dei dati personali, può trasferire in parte il trattamento dei dati raccolti su servizi cloud.

In ossequio alle indicazioni fornite dal Garante per la protezione dei dati personali, l' Istituto procederà a designare il fornitore dei servizi *cloud* quale Responsabile esterno del trattamento.

Il Titolare rileva che:

- ✓ nell'ambito delle valutazioni svolte nella identificazione dei cloud services:
  - ha effettuato verifiche sull'affidabilità del fornitore;
  - ha privilegiato i servizi che favoriscono la portabilità dei dati;
  - si è assicurato la disponibilità dei dati in caso di necessità;
  - ha effettuato verifiche sulla localizzazione dei server di stoccaggio dei dati;
  - ha effettuato verifiche sui tempi e modi di conservazione dei dati;
  - ha effettuato verifiche sulle modalità di archiviazione e trasmissione dei dati, privilegiando tecniche crittografiche, accompagnate da robusti meccanismi di identificazione dei soggetti autorizzati all'accesso;

- ha selezionato i dati da inserire nel *cloud*. Il Titolare ha identificato categorie di dati che devono essere connotate da un alto livello di sicurezza (c.d. *High Security Level*, HSL):

- ✓ nell'ambito dell'utilizzo dei c*loud services*, si assicura che siano adottate misure tecniche e organizzative volte a ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, di modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole;
- ✓ ha programmato una specifica formazione per il personale incaricato dei trattamenti dei dati mediante *cloud services* al fine di limitare rischi di accesso illecito, di perdita di dati o, più in generale, di accesso non consentito. L'attività di formazione riguarderà non solo gli elementi tecnici che consentono una scelta consapevole delle tecnologie cloud da adottare ma anche le fasi operative del trattamento.

4.4. DATA PROTECTION OFFICER

Il DPO svolge i seguenti compiti:

a. assiste il Titolare del trattamento nello svolgimento dei suoi adempimenti;
b. assiste il Titolare, il Responsabile e l'Amministratore di Sistema nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati, per quanto riguarda gli adempimenti derivanti dalla normativa in materia di riservatezza e protezione dei dati personali;
c. collabora con il Titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del registro delle attività di trattamento, in collaborazione con l'Amministratore di Sistema e con le altre unità della Istituto, nonché per gli eventuali aggiornamenti e adeguamenti del documento stesso;
d. vigila sull'osservanza del presente regolamento e fornisce consulenza ai Responsabili del trattamento sulle problematiche riguardanti la normativa privacy;
e. cura l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno della Istituto per l'applicazione del vigente Regolamento;
f. effettua i necessari approfondimenti per l'applicazione della normativa in materia di protezione dei dati personali, anche attraverso la costituzione di appositi gruppi di lavoro;

g. propone interventi di formazione a livello aziendale in tema di normativa sulla riservatezza e protezione dei dati;
h. effettua una ricognizione dei contratti in essere con i Responsabili esterni del trattamento dei dati previa informativa e comunicazione scritta da parte dei soggetti che stipulano accordi.

In ossequio a quanto disposto *dall'art. 37 Reg. 679/2016 e dalle "Linee-guida sui responsabili della protezione dei dati (RPD)" adottate il 13 dicembre 2016* – emendate e adottate in data 5 aprile 2017, il Titolare del trattamento HA ha designato un *Responsabile della protezione dei dati* (*Data Protection Officer*).

Detta designazione è STATA ritenuta opportuna in ragione delle attività principali svolte dal Titolare del trattamento che non richiedono il monitoraggio regolare e sistematico degli interessati su larga scala.

Ai fini della corretta interpretazione della locuzione "larga scala", il Gruppo di Lavoro Articolo 29 ha raccomandato di tenere conto, in particolare, dei fattori elencati nel prosieguo:

- ✓ il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- ✓ il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- ✓ la durata, ovvero la persistenza, dell'attività di trattamento;
- ✓ la portata geografica dell'attività di trattamento.

5. I DATI TRATTATI

L'Istituto nell'esercizio delle proprie attività tratta, in modo cartaceo e/o digitale, le seguenti categorie di dati relativi agli interessati:

1. Dati personali
2. Dati particolari
3. Dati Giudiziari

1. Dato Personale: si intende qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale 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" ai *sensi dell'art. 4 del Reg. n. 679/2016.*

2. Dato Sensibile: è il dato personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, e 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. Ai sensi dell'art. 9 GDPR è vietato trattare dati particolari salvo si verifichi uno dei seguenti casi:

a. l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
b. il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
c. il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la

fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

d. il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
   f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
   g) 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;

b. h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità,
   i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

c. j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. Dato giudiziario: è il dato rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679(articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza. 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.

5.1. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

L'*art. 5 del Reg. n. 679/2016* esprime i principi generali ai quali l' Istituto si è conformato con riguardo a qualsiasi processo aziendale che preveda il trattamento di dati personali. Tali principi sono:

a. Il principio di liceità, correttezza e trasparenza: un trattamento si considera lecito quando è conforme alla legge in generale e corretto quando avviene in maniera tale da rispettare la volontà di tutela.
b. Il principio di finalità del trattamento: richiede che ogni trattamento dei dati personali avvenga per finalità determinate, esplicite e legittime. Le finalità vanno rese note all'interessato, prima della raccolta dei dati, attraverso opportuna informativa.
c. Il principio di minimizzazione dei dati: ogni trattamento deve essere adeguato, pertinente e non eccedente cioè limitato a quanto necessario rispetto alle finalità per le quali i dati sono trattati.
d. Il principio di qualità ed esattezza dei dati trattati: richiede un'attenta verifica dei dati non solo al momento della loro raccolta presso l'interessato, ma anche in seguito con periodici aggiornamenti.
e. Il principio della giusta conservazione del trattamento: richiede che i dati siano conservati per il tempo necessario a realizzare le finalità per le quali sono stati raccolti. Questo principio intende ridurre i rischi privacy quali la distruzione o la perdita dei dati, gli accessi non autorizzati e la modifica dello scopo della raccolta.
f. Il principio di necessità: si configura riducendo al minimo l'utilizzazione dei dati personali, in modo da escluderne il trattamento quando le finalità possono essere perseguite mediante dati anonimi con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità.

6. TRATTAMENTI DEI DATI PERSONALI

Con l'espressione "**trattamento**" deve intendersi qualunque operazione o complesso di operazioni, compiute con o senza l'ausilio di processi automatizzati applicati a dati personali o all'insieme di dati personali, concernenti:

a. la **raccolta** dei dati;
b. la r**egistrazione** dei dati, cioè il loro inserimento su supporti, manuali o automatizzati, al fine di rendere i dati disponibili per successivi trattamenti;
c. l'**organizzazione** dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, ecc;
d. la **conservazione** dei dati alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
e. la **consultazione**;
f. l'**elaborazione**, ovvero le operazioni che attribuiscono significato ai dati in relazione allo scopo per i quali essi sono stati raccolti;
g. la **modificazione** dei dati registrati in relazione a variazioni o a nuove acquisizioni;
h. la **selezione**, l'**estrazione** e il **raffronto**;
i. l'**utilizzo**;
j. l'i**nterconnessione**, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
k. il **blocco**, cioè la conservazione dei dati con sospensione temporanea dei trattamenti;
l. la **comunicazione,** ovvero la trasmissione dei dati ad uno o più soggetti determinati;
m. la **diffusione**, ovvero il dare conoscenza dei dati personali a soggetti indeterminati;
n. la **cancellazione;**
o. la **distruzione**.

Il trattamento dei dati è consentito solo da parte del Titolare del trattamento, dei Responsabili e degli incaricati.

Il trattamento dei dati raccolti direttamente e/o indirettamente dalla Istituto è effettuato sia con strumenti cartacei che con strumenti automatizzati.

Il trattamento di particolari categorie di dati personali viene effettuato nel pieno rispetto dell'*art. 9 del Reg. n. 679/2016*.

7. REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

Il Titolare tiene un registro delle attività di trattamento svolte sotto la propria responsabilità, anche in qualità di responsabile esterno del trattamento. Tale registro contiene tutte le seguenti informazioni:

a. il nome e i dati di contatto del Titolare e del Responsabile della protezione dei dati;
b. le finalità del trattamento;
c. una descrizione delle categorie di interessati e delle categorie di dati personali;
d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
f. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

8. DATA PROTECTION IMPACT ASSESSMENT

La valutazione d'impatto dei trattamenti sulla protezione dei dati personali deve essere realizzata, prima di procedere al trattamento, dal Titolare del trattamento quando un tipo di trattamento, considerata la natura, il contesto, le finalità del trattamento, può prestare un rischio elevato per la sicurezza dei diritti e le libertà delle persone fisiche, sia in relazione al contesto fisico e ambientale di riferimento sia agli strumenti utilizzati.

Prioritariamente deve essere definito dal Titolare del trattamento l'elenco delle categorie di trattamenti soggette al requisito della valutazione d'impatto sulla protezione dei dati.

La valutazione deve contenere:

a. Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso l'interesse legittimo perseguito dal Titolare del trattamento;
b. Una valutazione delle necessità e delle proporzionalità dei trattamenti in relazione alle finalità;
c. Una valutazione dei rischi per i diritti e le libertà degli interessati;

d. Le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente Regolamento, tenuto conto dei diritti e degli interessati legittimi.

9. TRASFERIMENTO DATI ALL'ESTERO

Nei trasferimenti dei dati verso paesi extra UE, il Titolare del trattamento deve valutare attentamente le procedure e gli adempimenti derivanti dall'adozione di:

- ✓ Decisioni di adeguatezza: generalmente la trasmissione oltreconfine dei dati personali è consentita soltanto se il luogo al quale le informazioni vengono trasmesse garantisce un adeguato livello di protezione dei dati.
- ✓ Clausole contrattuali standard, strumento in grado di fornire garanzie appropriate che assicurano un livello adeguato di tutela.
- ✓ BCR – Binding Corporate Rules, ovvero regole in materia di privacy interne al gruppo societario multinazionale, che la capogruppo stabilita all'interno dell'UE adotta attraverso una dichiarazione unilaterale, rendendo questo regolamento vincolante per tutte le istituto collegate ad essa.

10. ALLEGATI