REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

ENGIM LOMBARDIA ETS

PRIMA EMISSIONE	25.05.2018
REVISIONE 01	25.07.2023

Sede legale ed operativa:
Valbrembo "Colli": via Sombreno 2 – 24030 Valbrembo (BG) – tel. 035 527853 / fax 035 339595 /
C.F. e P. Iva 03485690162 / e-mail info@engimlombardia.org / sito: lombardia.engim.org
Sedi operative:
Brembate "Centro": via IV Novembre 23 – 24030 Brembate Sopra (BG) – tel. / fax 035 332615
Brembate "Geller": via Donizetti 109/111 D1 – 24030 Brembate Sopra (BG) – tel. / fax 035 332087
Merate: viale Verdi 1 – 23807 Merate (LC) – tel. / fax 039 9419102

Registrazione n° 0312193

Sommario

TITOLO I - PRINCIPI E DISPOSIZIONI GENERALI

CAPO I - RIFERIMENTI NORMATIVI E AMBITO DI APPLICAZIONE

Articolo 1 - Oggetto

1. Il presente Regolamento e i relativi Allegati recano i principi e le disposizioni ai quali ENGIM LOMBARDIA ETS (di seguito ENGIM LOMBARDIA ETS o Ente) deve attenersi con riguardo alle attività di Trattamento dei Dati Personali come di seguito definiti.

Articolo 2 - Riferimenti normativi

1. Le principali fonti normative di riferimento sono costituite da:
   - 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 ("Regolamento Generale sulla Protezione dei Dati Personali");
   - D.Lgs. 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali", così come modificato e integrato dal D.Lgs. n. 101/2018, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 (regolamento generale sulla protezione dei dati)".
2. L'ENTE osserva altresì le Linee Guida e i Provvedimenti adottati dal Garante per la Protezione dei Dati Personali, i provvedimenti del Comitato Europeo per la Protezione dei Dati e il "Codice Etico e di Comportamento" dell'ENTE.

Articolo 3 - Ambito di applicazione soggettivo

1. Il presente Regolamento si applica a tutti coloro che svolgono attività di Trattamento dei Dati Personali di dipendenti/clienti/fornitori/studenti/famiglie– su supporto cartaceo e/o tramite procedure informatizzate – nell'ambito delle mansioni assegnate loro dall'ENTE.

Articolo 4 - Ambito di applicazione oggettivo

1. L'ENTE svolge attività di Trattamento dei Dati Personali nell'ambito delle proprie finalità. ENGIM LOMBARDIA ETS è una Fondazione ETS affiliata al Gruppo ENGIM, emanazione ed espressione carismatica ed operativa della Congregazione di San Giuseppe, che opera in Italia e nel Mondo attraverso la formazione, la cooperazione internazionale, l'orientamento e l'avviamento al lavoro per la crescita umana e professionale.
2. L'ENTE svolge i propri servizi nelle seguenti unità locali:

   VALBREMBO, Via Sombreno nr. 2

   GELLER, Via Donizetti 109/111, Padiglione D1, 24030 Brembate di Sopra

   CENTRO Via IV Novembre 23,24030 Brembate di Sopra

   MERATE, Viale Verdi 1, 23807

3. L'ENTE svolge attività di Trattamento dei Dati Personali sia come titolare del Trattamento che come Responsabile del Trattamento ex art. 28 GDPR nell'ambito di attività effettuate per conto di Regione Lombardia.

CAPO II – DEFINIZIONI

Articolo 5 - Definizioni

1. Ai fini del presente Regolamento si intende per:
   - "**ENTE**": l'ENTE in tutte le sue articolazioni;
   - "**Codice Privacy**": il D.Lgs. 30 giugno 2003 n. 196, "Codice in materia di protezione dei dati personali", così come modificato e integrato dal D.Lgs. n. 101/2018, recante "Disposizioni per l'adeguamento dell'ordinamento nazionale al 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", nonché da ss.mm.ii.;
   - **"GDPR"**: il 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; il Regolamento (UE) 2016/679 abroga la Direttiva 95/46/CE;
   - "**Dato Personale**": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**Interessato**"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
   - **"Categorie Particolari di Dati Personali"**: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, 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;
   - **"Dati Personali Comuni"**: dati personali che non appartengono alle categorie particolari di dati personali e non sono relativi a condanne penali e a reati o a connesse misure di sicurezza;
   - **"Dati Genetici"**: i dati 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;
   - **"Dati Biometrici**": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentano o confermino l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
   - **"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;
   - **"Dati Personali Giudiziari**": i dati personali relativi a condanne penali e reati o a connesse misure di sicurezza;
   - **"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;
   - **"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;
   - **"Pseudonimizzazione"**: il trattamento dei dati personali in modo tale che gli stessi 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;
   - **"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;

- **"Titolare del Trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **"Contitolare del Trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altro/i titolare/i del trattamento, determina le finalità e i mezzi del trattamento dei dati personali;
- **"Responsabile per la Protezione dei Dati"** o **"*Data Protection Officer*" ("RPD" o "DPO")**: figura indipendente che svolge attività di consulenza, supporto e controllo per il corretto adeguamento dell'ENTE al GDPR nonché di raccordo con il Garante per la Protezione dei Dati Personali;
- **"Responsabile del Trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **"Sub-Responsabile del Trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo a cui il responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento;
- **"Referente di Struttura"**: il Referente della Struttura nell'ambito della quale i dati personali sono gestiti per finalità istituzionali o in "conto terzi"; il Referente di Struttura è individuato sulla base della funzione organizzativa o carica istituzionale che ricopre ed esercita prevalentemente attività programmatiche e di controllo in relazione al trattamento dei dati personali all'interno della propria Struttura;
- **"Referente Interno":** Il Referente Interno agisce sulla base delle linee programmatiche determinate dal Referente di Struttura e si occupa di garantire la corretta gestione operativa dei dati personali;
- **"Sperimentatore Principale" o "*Principal Investigator*":** è il ricercatore responsabile del progetto di ricerca e delle attività compiute dagli altri ricercatori impegnati nello stesso;
- **"Autorizzato al Trattamento"**: chiunque agisca sotto l'autorità diretta del Titolare del Trattamento o del Responsabile del Trattamento che abbia accesso ai dati personali; non può trattare tali dati se non è istruito in tale senso dal Titolare del Trattamento;
- **"Autorità di controllo"**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del GDPR; in Italia l'autorità di controllo è il Garante per la Protezione dei Dati Personali;
- **"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;
- **"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 gli Autorizzati al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;
- **"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 considerati 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;
- **"Violazione dei dati personali"**: l'evento 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;
- **"Comunicazione"**: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dell'Unione europea, dal Responsabile o dal

suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate ai sensi dell'art. 2-*quaterdecies* del Codice Privacy, al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

- **"Diffusione"**: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

CAPO III - PRINCIPI GENERALI

Articolo 6 - Principi generali applicabili al Trattamento dei Dati Personali

1. L'ENTE tratta i Dati Personali nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento al rispetto della riservatezza e dell'identità personale. In particolare, l'ENTE svolge le attività di Trattamento dei Dati Personali nel rispetto dei principi previsti dall'art. 5, c. 1 del GDPR, ovvero i Dati Personali sono:
   - trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato ("principio di liceità, correttezza e trasparenza");
   - 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 considerato incompatibile con le finalità iniziali ("limitazione delle finalità");
   - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("principio di minimizzazione dei dati");
   - 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 ("principio di esattezza");
   - conservati in una forma che consenta l'identificazione degli Interessati per un arco temporale non superiore a quello necessario per il 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, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'Interessato ("principio di limitazione della conservazione");
   - trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante adeguate misure tecniche e organizzative da Trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("principio di integrità e riservatezza").

Articolo 7 - Principio di responsabilizzazione ("Accountability")

1. L'ENTE, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del Trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il Trattamento è effettuato conformemente alle prescrizioni del GDPR ("**principio di responsabilizzazione**").

Articolo 8 - Principi di privacy by design e privacy by default

1. L'ENTE, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del Trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal Trattamento, sia al momento di determinare i mezzi del Trattamento, sia all'atto del Trattamento stesso, mette in atto misure tecniche e organizzative

adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel Trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli Interessati ("principio di *privacy by design*").

2. L'ENTE mette in atto le misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i Dati Personali necessari per ogni specifica finalità di Trattamento. Tale obbligo vale per la quantità dei Dati Personali raccolti, la portata del Trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili Dati Personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica ("principio di privacy by default").

Articolo 9 - Basi giuridiche del Trattamento dei Dati Personali Comuni

1. L'ENTE tratta i Dati Personali solo in presenza di una base giuridica che renda lecito tale Trattamento.
2. L'ENTE, con la collaborazione del DPO, individua la corretta base giuridica per le attività di Trattamento e conserva la documentazione relativa all'individuazione della corretta base giuridica, che metterà a disposizione, su richiesta, al Garante per la Protezione dei Dati Personali.
3. Le basi giuridiche del trattamento individuate per i trattamenti svolti da ENGIM LOMBARDIA ETS sono indicate all'interno del registro del trattamento.

Articolo 10 - Basi giuridiche del Trattamento per Categorie Particolari di Dati Personali

1. Il Trattamento di Categorie Particolari di Dati Personali da parte dell'ENTE potrà essere effettuato solo nei casi indicati dalla legge o dal Reg. UE 679/16.
2. Le basi giuridiche del trattamento individuate per i trattamenti di dati particolari svolti da ENGIM LOMBARDIA ETS sono indicate all'interno del registro del trattamento.

Articolo 11 - Basi giuridiche del Trattamento per i Dati Personali Giudiziari

1. Il Trattamento dei Dati Personali Giudiziari da parte dell'ENTE è lecito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare:
   - l'adempimento di obblighi e l'esercizio di diritti da parte del Titolare del Trattamento o dell'Interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dall'art. 9, c. 2, lett. b), e dall'art. 88 del GDPR;
   - l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;
   - l'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
   - l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   - l'adempimento di obblighi derivanti dal D.lgs 39/2014 c.d. "antipedofilia"
   - l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;
   - l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
   - l'attuazione della disciplina in materia di attribuzione del *rating* di legalità delle imprese ai sensi dell'art. 5-*ter* del Decreto Legge 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla Legge 24 marzo 2012, n. 27;
   - l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Articolo 12 - Principi generali riguardanti l'esecuzione di un compito di interesse pubblico

1. Il Trattamento dei Dati Personali Comuni da parte dell'ENTE, la cui base giuridica è rappresentata dall'art. 6, c. 1, lett. e), del GDPR, può avvenire quando il "compito di interesse pubblico" è regolato da una norma di legge o, nei casi previsti dalla legge, di regolamento (in particolare per la Comunicazione e la Diffusione di Dati Personali si faccia riferimento al TITOLO II, Capo IV del presente Regolamento).
2. Il Trattamento di Categorie Particolari di Dati Personali da parte dell'ENTE, la cui base giuridica è rappresentata dall'art. 9, c. 2, lett. g), del GDPR, può avvenire quando il "compito di interesse pubblico rilevante" è regolato dal diritto dell'Unione europea, da una norma di legge o, nei casi previsti dalla legge, di regolamento che specifichi i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato. L'art. 2-*sexies*, c. 2, lett. bb) del Codice Privacy riconosce espressamente le attività di Trattamento svolte nel campo "dell'istruzione e formazione in ambito scolastico, professionale, superiore o universitario" come attività compiute in esecuzione di un compito di interesse pubblico rilevante. Inoltre, l'art. 2-*sexies*, c. 2 lett. cc) del Codice Privacy riconosce quali attività di Trattamento compiute in esecuzione di un compito di interesse pubblico "*i trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché' per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale*".

Articolo 13 - Principi generali riguardanti il Consenso dell'Interessato

1. L'ENTE ottiene il Consenso dell'Interessato quando lo stesso costituisce base giuridica idonea per le attività di Trattamento.
2. Per essere considerato valido, il Consenso deve consistere in una manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva indubbia, affinché i Dati Personali che lo riguardano siano oggetto di Trattamento; il Consenso, inoltre, deve essere dimostrabile.
3. Il Consenso si applica a tutte le attività di Trattamento svolte per la stessa o le stesse finalità. Qualora il Trattamento abbia più finalità, il Consenso deve essere prestato per tutte queste.
4. Il Consenso al Trattamento dei Dati Personali Comuni è validamente prestato solo qualora l'Interessato abbia preventivamente preso visione dell'informativa.
5. Il Consenso dell'Interessato dovrà essere, invece, necessariamente esplicito nei seguenti casi: (i) attività di Trattamento dei Dati Personali a fini di Profilazione, che produca effetti giuridici per l'interessato o conseguenze analoghe; (ii) Trattamento di Categorie Particolari di Dati Personali; (iii) trasferimento dei dati verso paesi terzi (ad esempio, extra Unione europea) o verso una organizzazione internazionale.
6. Il Consenso non è validamente prestato in caso di: (i) caselle preselezionate e (ii) silenzio e/o inattività dell'Interessato.
7. Il Consenso al Trattamento dei Dati Personali deve essere raccolto separatamente da quello prestato per altre attività.
8. Quando il Consenso costituisce la base giuridica che legittima le attività di Trattamento, ciascun autorizzato provvede a raccoglierlo e a conservare la relativa documentazione, composta dall'informativa resa all'interessato e dalla documentazione comprovante la manifestazione del consenso stesso, in modo da poter dimostrare tale adempimento.

TITOLO II - TRATTAMENTO DEI DATI PERSONALI

CAPO I - ORGANIZZAZIONE E RESPONSABILITA'

Articolo 14 - Titolare del Trattamento

1. Il Titolare del trattamento (data controller) è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le* **finalità** *e i* **mezzi** *del trattamento di dati personali*" (art. 4. par. 1, n. 7 GDPR). Come previsto dalla normativa sono previsti una serie di obblighi tra cui a titolo esemplificativo e non esaustivo:
   - individua e prende decisioni in ordine alle finalità ed alle modalità di trattamento dei dati personali, ivi compreso il profilo della sicurezza
   - tratta i dati in modo lecito, corretto e trasparente
   - garantisce il rispetto dei diritti degli interessati
   - adotta le misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione la tutela dei dati personali (privacy by design e by default)
   - effettua il censimento ed aggiorna l'elenco dei trattamenti dei dati personali in Ente e garantisce il diritto d'accesso come previsto dalle norme sulla privacy;
   - nomina con proprio atto gli autorizzati del trattamento dei dati personali, impartendo ad essi i compiti e le istruzioni,
   - nomina un Data Protection Officer (nei casi previsti dalla legge)
   - nomina i responsabili esterni al trattamento dei dati personali ex art. 28 GDPR 679/16;
   - elabora il registro del Trattamento
   - 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;
   - dispone verifiche periodiche per riesaminare e aggiornare le istruzioni impartite e le predette misure di sicurezza ogni qualvolta lo ritenga necessario;
   - redige, aggiorna e conserva le disposizioni Enteli in tema di Privacy.
2. Il Titolare del Trattamento è ENGIM LOMBARDIA ETS con sede legale a Valbrembo (BG) in Via Sombreno, 2 nella persona del legale rappresentante pro tempore,
3. Nei casi in cui il legale rappresentante, anche a seguito di attività di controllo e *audit*, rilevi comportamenti difformi a quanto previsto nel presente Regolamento, definisce, con la collaborazione del DPO, i necessari interventi correttivi e ne dispone l'attuazione.

Articolo 15 – Designato al trattamento

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.
3. Il soggetto è designato con apposito atto di nomina sottoscritto dal legale rappresentante ed è responsabile /degli adempimenti indicati nel presente Regolamento.

Articolo 16 - Autorizzati al Trattamento

1. Tutto il personale dipendente appartenente a ciascuna area, i collaboratori e gli eventuali altri soggetti che intrattengono rapporti di lavoro/collaborazione con l'ENTE nello svolgimento di compiti assegnati dall'ENTE stessa saranno Autorizzati al Trattamento, con apposito atto di nomina.
2. Gli Autorizzati al Trattamento:

- devono osservare le disposizioni contenute nel presente Regolamento e nelle regole operative applicabili;
- devono effettuare il Trattamento in osservanza delle misure di sicurezza adottate dall'ENTE
-ricevono formazione in materia di protezione dei Dati Personali specifica per l'area di appartenenza

Articolo 17 - Responsabile della Protezione dei Dati o Data Protection Officer ("RPD" o "DPO")

1. L'ENTE nomina un Responsabile della Protezione dei Dati o *Data Protection Officer* ("RPD" o "DPO"), soggetto di supporto al Titolare del Trattamento con funzioni di raccordo con il Garante per la Protezione dei Dati Personali.
2. Il DPO è designato in funzione delle qualità professionali e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere ai propri compiti.
3. Il DPO può essere un Dirigente dell'ENTE – o comunque una figura interna dotata di particolari competenze – o un soggetto esterno con incarico affidato sulla base di un contratto di servizi. Il DPO svolge i seguenti compiti:
   a) informare e fornire consulenza al Titolare del Trattamento, in merito agli obblighi derivanti dal presente Regolamento nonché dalla normativa europea e nazionale relativa alla protezione dei Dati Personali;
   b) sorvegliare l'osservanza del presente Regolamento e di altre disposizioni derivanti dalla normativa europea e nazionale relative alla protezione dei dati nonché delle politiche del Titolare del Trattamento o del Responsabile del Trattamento in materia di protezione dei Dati Personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione degli Autorizzati al Trattamento; in particolare, il DPO organizza incontri di formazione *ad hoc* con i componenti delle varie aree Enteli.
   c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
   d) cooperare con il Garante per la Protezione dei Dati Personali;
   e) fungere da punto di contatto per il Garante per la Protezione dei Dati Personali per questioni connesse al Trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
   f) collaborare alla redazione e all'aggiornamento dei registri del Trattamento;
   g) svolgere ogni ulteriore compito attribuitogli dal Titolare del Trattamento solo se compatibile con le sue funzioni e il suo ruolo.
4. Nell'eseguire i propri compiti, il DPO considera debitamente i rischi inerenti al Trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
5. Al DPO sono garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della relativa funzione.
6. Il DPO ha ampio accesso alle informazioni ed è interpellato per ogni problematica inerente la protezione dei Dati Personali nonché consultato per ogni nuovo Trattamento che si intende avviare, fin dalla progettazione dello stesso.
7. L'ENTE garantisce che il DPO eserciti le proprie funzioni in autonomia e indipendenza e, in particolare, non assegna allo stesso attività o compiti che risultino in contrasto o conflitto di interessi.
8. Il DPO non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati ai sensi dell'art. 39 del GDPR.
9. L'ENTE non rimuove o penalizza il DPO in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni.
10. L'Ente ha nominato il DPO nella persona dell'avv. Laura Lussu.Il nominativo e i dati di contatto del DPO sono stati comunicati al Garante per la Protezione dei Dati Personali. I dati di contatto del DPO sono inseriti nelle informative e pubblicati sul sito internet istituzionale www.lombardia.engim.org

Articolo 18 – Responsabile esterno del Trattamento

1. Qualunque soggetto esterno che esegua – in base a un contratto, una convenzione o altro atto giuridico – attività di Trattamento dei Dati Personali per conto del Titolare del Trattamento deve essere designato Responsabile del Trattamento ai sensi dell'art. 28 del GDPR.

2. Il Responsabile del Trattamento è nominato con apposito atto del Titolare del Trattamento e fornisce adeguate garanzie, in particolare, per quanto riguarda le misure tecniche e organizzative atte a consentire il rispetto delle disposizioni del GDPR e la tutela dei diritti dell'Interessato.
3. Il Responsabile del Trattamento risponde per l'eventuale danno causato dal Trattamento solo se non ha adempiuto alle prescrizioni del GDPR specificatamente allo stesso indirizzate o ha agito in modo difforme o contrario rispetto alle istruzioni impartite dal Titolare del Trattamento. Il Responsabile del Trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. Il Responsabile del Trattamento risponde in solido con il Titolare del Trattamento al fine di garantire il risarcimento effettivo del danno patito dall'Interessato. Qualora il Titolare del Trattamento o il Responsabile del Trattamento abbia pagato, conformemente all'art. 82, c. 4, del GDPR, l'intero risarcimento del danno, quest'ultimo ha diritto di reclamare dall'altro soggetto coinvolto nello stesso Trattamento la parte del risarcimento corrispondente alla sua parte di responsabilità, conformemente alle condizioni di cui all'art. 82, c. 2, del GDPR.
5. Il Responsabile del Trattamento che non rispetti o ecceda nelle attività di Trattamento le istruzioni a lui impartite dal Titolare del Trattamento diventa, a sua volta, Titolare del Trattamento per la parte delle attività relative ai Dati Personali non previste nell'atto di nomina.

Articolo 19 - Sub-Responsabile del Trattamento

1. Il Responsabile del Trattamento può ricorrere ad altro Responsabile del Trattamento ("Sub-Responsabile") per l'esecuzione di specifiche attività di Trattamento per conto del Titolare del Trattamento, previa autorizzazione scritta di quest'ultimo, specifica o generale, mediante contratto o altro atto giuridico con il quale vengano imposti gli stessi obblighi in materia di protezione dei dati contenuti nel contratto tra il Titolare del Trattamento e il Responsabile del Trattamento.
2. Il Responsabile del Trattamento risponde dinanzi al Titolare del Trattamento dell'inadempimento del Sub-Responsabile, anche ai fini del risarcimento di eventuali danni causati.

Articolo 20 - Contitolari del Trattamento

1. Quando uno o più Titolari del Trattamento determinano congiuntamente con l'ENTE le finalità e i mezzi del Trattamento, gli stessi sono Contitolari del Trattamento.
2. L'ENTE stipula con il Contitolare del Trattamento un accordo che determini i rispettivi ruoli, rapporti e responsabilità ai fini dell'osservanza della normativa, ai sensi dell'art. 26 del GDPR.
3. L'Interessato può esercitare i diritti riconosciuti dal GDPR nei confronti di ciascun Contitolare del Trattamento.

Articolo 21 - Autorità di controllo

1. L'Autorità di controllo di riferimento per l'ENTE è il Garante per la Protezione dei Dati Personali.

CAPO II - ADEMPIMENTI

Articolo 22 - Informativa

1. Nel rispetto del principio di trasparenza, per ogni tipologia di Trattamento di Dati Personali l'ENTE fornisce agli Interessati un'apposita informativa.
2. L'informativa deve essere concisa, trasparente, intellegibile, facilmente accessibile e redatta con un linguaggio chiaro e semplice. Le informazioni sono fornite per iscritto o con altri mezzi, anche elettronici. L'Interessato potrà chiedere che le informazioni siano fornite oralmente, purché sia comprovata l'identità dell'Interessato.
3. Se i dati vengono raccolti presso l'Interessato, l'ENTE fornisce l'informativa agli Interessati al momento della raccolta dei dati. È necessario rendere agli Interessati una nuova informativa quando il Titolare del Trattamento intenda trattare i dati già acquisiti per una finalità diversa da quella per cui sono stati raccolti ovvero vengano

modificati elementi fondamentali del Trattamento originario rappresentato agli Interessati.

4. Se i Dati Personali vengono raccolti presso Terzi, ciascuna area fornisce l'informativa agli Interessati (i) al momento della prima comunicazione con gli stessi, nel caso in cui i Dati Personali siano destinati alla comunicazione con l'Interessato (ad esempio, invio di una *newsletter*), (ii) al momento della comunicazione prima ad altro destinatario ovvero, negli altri casi, entro un termine ragionevole dall'ottenimento dei Dati Personali, ma, al più tardi, entro un mese, in considerazione delle specifiche circostanze in cui i Dati Personali sono trattati. Non si dovrà fornire l'informativa nei seguenti casi: (i) l'Interessato dispone già delle informazioni;

(ii) comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato (la documentazione che illustra i motivi per cui si è ritenuto che lo sforzo fosse sproporzionato deve essere conservata dalla Struttura e, su richiesta, messa a disposizione del Garante per la Protezione dei Dati Personali); (iii) l'ottenimento dei dati o la comunicazione degli stessi sono previsti espressamente dal diritto europeo o nazionale; (iv) qualora i Dati Personali debbano rimanere riservati, conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o nazionale, compreso un obbligo di segretezza previsto per legge.

5. L'informativa deve contenere:
   - l'identità e i dati di contatto del Titolare del Trattamento;
   - i dati di contatto del Responsabile della Protezione dei Dati;
   - le finalità e la base giuridica del Trattamento;
   - le categorie di Dati Personali raccolte, e, nei casi in cui i dati non siano stati direttamente conferiti dall'Interessato, anche la fonte da cui hanno origine i Dati Personali e l'eventualità che i dati provengano da fonti accessibili al pubblico;
   - gli eventuali destinatari o le eventuali categorie di destinatari dei Dati Personali;
   - ove applicabile, l'intenzione del Titolare del Trattamento di trasferire i Dati Personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'art. 46 o 47, o all'art. 49 del GDPR, il riferimento alle garanzie appropriate od opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili;
   - il periodo di conservazione dei Dati Personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   - i diritti che l'Interessato può esercitare, quali l'accesso ai Dati Personali, la rettifica o la cancellazione degli stessi, la limitazione del Trattamento dei dati che lo riguardano o l'opposizione al Trattamento degli stessi; il diritto alla portabilità dei dati, il diritto di proporre reclamo al Garante per la Protezione dei Dati Personali; qualora il Trattamento sia basato sull'art. 6, c. 1, lett. a), oppure sull'art. 9, c. 2, lett. a), il diritto di revocare il Consenso in qualsiasi momento senza pregiudicare la liceità del Trattamento basata sul Consenso prestato prima della revoca (nei casi in cui i dati siano stati direttamente conferiti dall'Interessato nel momento in cui i Dati Personali sono ottenuti); qualora il Trattamento sia basato sull'art. 6, c. 1, lett. e), deve essere esplicitamente portato all'attenzione dell'Interessato e presentato chiaramente e separatamente da qualsiasi altra informazione il diritto di opporsi in qualsiasi momento al Trattamento dei Dati Personali che lo riguardano effettuato per tali finalità;
   - se la comunicazione dei 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 (nei casi in cui i dati siano stati direttamente conferiti dall'Interessato nel momento in cui i Dati Personali sono ottenuti);

     l'esistenza di un processo decisionale automatizzato, compresa la Profilazione, e la logica utilizzata, nonché l'importanza e le conseguenze previste da tale Trattamento per l'Interessato (nei casi in cui i dati siano stati direttamente conferiti dall'Interessato, nel momento in cui i Dati Personali sono ottenuti).

6. Gli Autorizzati al Trattamento possono trattare i Dati Personali solo per le specifiche finalità indicate nell'informativa fornita all'Interessato.

Articolo 23 - Registro delle attività di Trattamento

1. L'ENTE, quale Titolare del Trattamento, istituisce e aggiorna il Registro delle attività di Trattamento, che descrive le attività di Trattamento svolte presso l'ENTE e ne delinea le principali caratteristiche. Il Registro può essere tenuto sia in formato elettronico che cartaceo.
2. Il Registro delle attività di Trattamento, redatto dall'ENTE quale Titolare del Trattamento, deve contenere le seguenti informazioni:
   - dati identificativi e di contatto dell'ENTE, degli eventuali Contitolari e del DPO;
   - le finalità del Trattamento;
   - la descrizione delle categorie degli Interessati e delle categorie di Dati Personali;
   - le categorie di destinatari, a cui i Dati Personali sono stati o saranno comunicati, compresi destinatari di paesi terzi od organizzazioni internazionali;
   - l'eventuale trasferimento di Dati Personali verso un paese terzo o un'organizzazione internazionale, indicando i dati identificativi del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art. 49, c. 2, del GDPR, la documentazione delle garanzie adeguate;
   - ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   - ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate, di cui all'art. 32, c. 1, del GDPR.
3. L'ENTE istituisce e aggiorna, inoltre, il Registro delle attività di Trattamento in qualità di Responsabile del Trattamento, nel quale sono descritte le attività di Trattamento svolte in qualità di Responsabile per conto di altri Titolari del Trattamento.
4. Il Registro delle attività di Trattamento, redatto dall'ENTE quale Responsabile del Trattamento, deve contenere le seguenti informazioni:
   - dati identificativi e di contatto dell'ENTE, del Titolare del Trattamento, di eventuali altri Responsabili del Trattamento e del DPO dell'ENTE e del Titolare del Trattamento per conto del quale agisce l'ENTE;
   - le categorie di Trattamenti effettuati per conto di ogni Titolare del Trattamento;
   - l'eventuale trasferimento di Dati Personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale, e, per i trasferimenti di cui all'art. 49, c. 2, del GDPR, la documentazione delle garanzie adeguate;
   - ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate di cui all'art. 32, c. 1, del GDPR.
5. Il Titolare del Trattamento redige i predetti Registri delle attività di Trattamento, in collaborazione con il DPO, e ne cura periodicamente l'aggiornamento. I Registri delle attività di Trattamento devono essere tenuti a disposizione del Garante per la Protezione dei Dati Personali.

Articolo 24 - Valutazione di impatto

1. L'ENTE effettua una valutazione di impatto quando le attività di Trattamento dei Dati Personali che prevedono in particolare l'utilizzo di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del Trattamento, possono presentare un rischio elevato per i diritti e le libertà dell'Interessato.
2. L'art. 35 del GDPR specifica che la valutazione di impatto è obbligatoria nei casi seguenti:
   - valutazione sistematica e globale degli aspetti personali relativi a persone fisiche, basata su un Trattamento automatizzato, compresa la Profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
   - Trattamento, su larga scala, di Categorie Particolari di Dati Personali, quali l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di 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, dati relativi a condanne penali e a reati o a connesse misure di sicurezza;
   - sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza).

3. L'ENTE, con la collaborazione delle aree e del DPO, determinerà i casi nei quali si rende necessario procedere a una valutazione di impatto nel rispetto di quanto previsto dalle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017 e modificate il 4 ottobre 2017, nonché il provvedimento n. 467 dell'11 ottobre 2018 (9058979) del Garante per la Protezione dei Dati Personali.
4. Qualora un'AREA ritenesse di trovarsi in uno dei suddetti casi, consulterà il DPO per decidere se effettuare la valutazione di impatto. La decisione deve essere documentata per iscritto e conservata per poter essere prodotta in caso di richiesta da parte del Garante per la Protezione dei Dati Personali.
5. Nei casi in cui, al termine della valutazione di impatto e dell'adozione delle misure di sicurezza, si ritenesse che le attività di Trattamento comportino un rischio elevato per gli Interessati, il Titolare del Trattamento, in collaborazione con il DPO, procederà a consultare il Garante per la Protezione dei Dati Personali ai sensi dell'art. 36 del GDPR.

CAPO III - DIRITTI DELL'INTERESSATO

Articolo 25 - Diritti dell'Interessato

1. L'ENTE garantisce il rispetto dei diritti degli Interessati disciplinati dagli artt. 12-22 del GDPR, ove applicabili, e, in particolare, di:
   - essere informati circa le attività di Trattamento svolte sui propri Dati Personali tramite l'informativa ("diritto a essere informato") (vedasi art. 22 del presente Regolamento);
   - avere conferma dal Titolare del Trattamento che sia o meno in corso un'attività di Trattamento sui propri Dati Personali e ottenere l'accesso a tali dati ("diritto di accesso ai dati personali");
   - ottenere la rettifica dei dati inesatti e l'integrazione dei dati incompleti ("diritto alla rettifica");
   - ottenere la cancellazione dei propri Dati Personali ("diritto all'oblio");
   - ottenere la limitazione al trattamento dei propri dati ("diritto alla limitazione");
   - ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i relativi Dati Personali forniti a un Titolare del Trattamento e trasmettere tali dati a un altro Titolare del Trattamento senza impedimenti da parte del Titolare del Trattamento cui li ha forniti ("diritto alla portabilità");
   - opporsi in qualsiasi momento, per motivi connessi alla propria situazione particolare, al Trattamento dei propri Dati Personali ai sensi dell'art. 6, c. 1, lett. e) o f), del GDPR, compresa la Profilazione ("diritto all'opposizione");
   - non essere sottoposto a una decisione basata unicamente sul Trattamento automatizzato, compresa la Profilazione, che produca effetti giuridici nei confronti dell'interessato stesso o che incida in modo analogo significativamente sulla propria persona, fatti salvi i casi in cui ciò è previsto dalla legge ("diritto a non essere sottoposti a trattamento automatizzato").
2. L'Interessato presenta istanza di esercizio dei diritti all'Ente o al DPO, senza alcuna formalità, previa dimostrazione della propria identità.
3. L'ENTE risponde tempestivamente alle richieste di esercizio dei diritti e, comunque, entro 30 GIORNI dal ricevimento dell'istanza. Tale termine può essere prorogato di ulteriori due mesi (per un totale di tre mesi), tenuto conto della complessità e del numero delle richieste. In ogni caso, l'ENTE dovrà comunicare tale proroga all'Interessato entro un mese dal ricevimento dell'istanza, indicando i motivi del ritardo.
4. L'ENTE può negare la risposta a una richiesta di esercizio dei diritti solo nel caso in cui quest'ultima risulti manifestamente infondata o eccessiva, in particolare per il suo carattere ripetitivo; sarà onere dell'ENTE dimostrare il carattere manifestamente infondato o eccessivo della richiesta e comunicare i motivi del diniego all'Interessato.
5. L'ENTE non richiede un contributo spese per dare riscontro a richieste di esercizio dei diritti, fatti salvi i casi di istanze manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo.

CAPO IV – CIRCOLAZIONE, COMUNICAZIONE, DIFFUSIONE E TRASFERIMENTO DI DATI PERSONALI

Articolo 26 - Circolazione dei Dati Personali all'interno dell'ENTE

1. L'accesso ai Dati Personali da parte del personale dell'ENTE è ispirato al principio del *need- to-know*: le informazioni devono essere rese disponibili esclusivamente ai soggetti che hanno necessità di accedervi, per lo svolgimento dell'attività lavorativa, mediante strumenti, sia cartacei sia informatici, atti a facilitarne la fruizione.

Articolo 27 - Comunicazione dei Dati Personali al di fuori dell'ENTE

1. La comunicazione dei Dati Personali al di fuori dell'ENTE può avvenire solo ove sussista una specifica base giuridica (vedasi artt. 10, 11, 12 e 13 del presente Regolamento).
2. Ogni richiesta, rivolta da soggetti esterni all'ENTE, finalizzata a ottenere la comunicazione di Dati Personali, salvi i casi espressamente previsti da una norma di legge o regolamento, deve essere sottoposta per iscritto e motivata; l'accoglibilità della richiesta sarà valutata dal Titolare in collaborazione con il DPO.

Articolo 28 - Diffusione dei Dati Personali

1. La diffusione dei Dati Personali può avvenire solo ove prevista da una norma di legge applicabile alla fattispecie concreta ovvero sia stato rilasciato il consenso da parte dell'Interessato.

Articolo 29 - Trasferimento di Dati Personali verso paesi terzi od organizzazioni internazionali

1. Il trasferimento di Dati Personali verso un paese terzo o un'organizzazione internazionale avviene sulla base di una delle misure adeguate previste dal Capo V del GDPR, quali:
   - decisione di adeguatezza adottata a norma dell'art. 45, c. 3, del GDPR e delle decisioni adottate sulla base dell'art. 25, c. 6, della Direttiva 95/46/CE;
   - uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche od organismi pubblici;
   - le norme vincolanti di impresa;
   - le clausole contrattuali standard adottate dalla Commissione Europea o da un'Autorità di controllo e approvate dalla Commissione Europea secondo la procedura d'esame di cui all'art. 93, c. 2, del GDPR;
   - un codice di condotta approvato a norma dell'art. 40 del GDPR, unitamente all'impegno vincolante ed esecutivo da parte del Titolare del Trattamento o del Responsabile del Trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati;
   - un meccanismo di certificazione approvato a norma dell'art. 42 del GDPR, unitamente all'impegno vincolante ed esigibile da parte del Titolare del Trattamento o del Responsabile del Trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli Interessati.
   - Il trasferimento di Dati Personali che non può basarsi su una decisione di adeguatezza o su una garanzia adeguata, che si verifica in condizioni particolari e in casi di trasferimenti sporadici, può avvenire ove ricorra una delle seguenti condizioni:
   - l'Interessato ha esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
   - il trasferimento è necessario all'esecuzione di un contratto concluso tra l'Interessato e il Titolare del Trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'Interessato;
   - il trasferimento è necessario per la conclusione o l'esecuzione di un contratto stipulato tra il Titolare del Trattamento e un'altra persona fisica o giuridica a favore dell'Interessato;
   - il trasferimento è necessario per importanti motivi di interesse pubblico;

- il trasferimento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- il trasferimento è necessario per tutelare gli interessi vitali dell'Interessato o di altre persone, qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio Consenso;
- il trasferimento è effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

2. Nel caso di trasferimento di Dati Personali verso un paese terzo o un'organizzazione internazionale, ciascuna area individua, in collaborazione con il DPO, l'idonea misura per garantire la tutela dei Dati Personali.

TITOLO III - MISURE DI SICUREZZA E NOTIFICA DI VIOLAZIONE DEI DATI PERSONALI

Articolo 30 - Misure di sicurezza

1. L'ENTE adotta misure di sicurezza, tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del Trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
2. Le misure sono individuate in collaborazione con il Titolare del Trattamento e con il supporto del DPO.
3. Ciascun dipendente o collaboratore è responsabile del rispetto delle misure tecniche individuate dall'Area Sistemi Informatici, in collaborazione con il Titolare del Trattamento e con il supporto del DPO.

Articolo 31 - Conservazione dei Dati Personali

1. L'ENTE conserva i Dati Personali solo per il tempo necessario al conseguimento delle finalità del Trattamento e/o per il periodo indicato dalla legge. Adeguate misure di sicurezza vengono adottate per assicurare la sicurezza dei Dati Personali durante la loro conservazione.
2. Al termine del periodo di conservazione, i Dati Personali vengono cancellati, distrutti o resi anonimi.
3. Il periodo di conservazione dei Dati Personali oggetto di Trattamento è individuato nel registro del trattamento.

Articolo 32 - Violazione dei Dati Personali ("*Data Breach*")

1. Per la gestione degli incidenti di sicurezza e delle Violazioni dei Dati Personali si rimanda a quanto stabilito nella procedura per la gestione dei data breach.

TITOLO IV - CONTROLLI, SANZIONI E DISPOSIZIONI FINALI

Articolo 33 - Controlli ammessi

1. Il Titolare del Trattamento o altri soggetti da quest'ultimo delegati hanno facoltà di effettuare controlli, circa l'adozione delle corrette misure per garantire il rispetto dei diritti e delle libertà fondamentali degli Interessati, i cui Dati Personali sono oggetto di Trattamento da parte dell'ENTE.
2. I controlli possono avere a oggetto anche le risorse informatiche messe a disposizione dall'ENTE, nel rispetto di quanto disposto dal regolamento informatico.

Articolo 34 - Sanzioni

1. I comportamenti in violazione della normativa vigente in tema di protezione dei Dati Personali, del presente Regolamento, dei suoi Allegati e delle regole operative che hanno una rilevanza disciplinare sono sanzionati secondo le forme e le modalità previste dal Contratto collettivo, fermi restando i diversi profili di responsabilità

civile e penale e amministrativa.

Articolo 35 - Aggiornamento del presente Regolamento e relativi Allegati

1. Il presente Regolamento potrà essere aggiornato a seguito di:
   - modifiche normative sopravvenute;
   - introduzione di nuove pratiche volte a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
   - inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.
2. Le eventuali modifiche e/o gli eventuali aggiornamenti degli Allegati del presente Regolamento non costituiscono modifica di quest'ultimo.

ENGIM LOMBARDIA ETS

ALLEGATI

1. Organigramma
2. Registro del trattamento ex art. 30 GDPR
3. Registro del responsabile del trattamento
4. Informative (candidatura, dipendenti,, tirocinanti/stagisti, collaboratori, formazione finanziata RL, formazione autofinanziata, servizi al lavoro)
5. Nomina autorizzato al trattamento
6. Informativa fornitori
7. Nomine responsabili al trattamento ex art. 28 GDPR
8. Nomina responsabile esterno ENGIM LOMBARDIA ETS
9. Nomina amministratori di sistema
10. Regolamento informatico
11. Vademecum Trattamento Dati

PROCEDURE

12. P01 Archiviazione Cartacea
13. P02 Archiviazione consensi
14. P03 Procedura di Verifica
15. P04 Procedura data Breach
16. P05 Procedura diritti Interessati
17. P06 Procedura visite Ispettive
18. P07 Procedura On Boarding e off Boarding