Gruppo di Azione Locale BALDO – LESSINIA

Via Giulio Camuzzoni, 8 – 37038 Soave (VR)

GAL BALDO LESSINIA
AGENZIA DI SVILUPPO

VERBALE DEL CONSIGLIO DI AMMINISTRAZIONE

COPIA Deliberazione n. 36 del 13 giugno 2022

OGGETTO	PSL GAL Baldo-Lessinia 2014/2020 - Misura 19 del PSR Veneto 2014/2020 "Sostegno allo sviluppo locale LEADER" – **Approvazione Revisione in ambito Privacy per il GAL Baldo-Lessinia.**

In data 13 GIUGNO 2022 alle ore 18:30, presso la sede del GAL Baldo-Lessinia, si è riunito il Consiglio di Amministrazione nelle persone dei Sigg.

Cognome Nome	Carica	Ente rappresentato	Componente	Presente	Assente
Anselmi Ermanno	Presidente	Coldiretti di Verona, Confederazione Italiana Agricoltori	Priv/parti econ. e soc.	X	
Rossi Paolo	Vicepresidente	BIM Adige	Pubblico	X	
Storti Ercole	Consigliere	Comune di San Giovanni Ilarione	Pubblico		X
Pazzocco Dennis	Consigliere	Comune di Roverè Veronese	Pubblico	X	
Campostrini Raffaello	Consigliere	Comune di Sant'Anna d'Alfaedo	Pubblico	X	
Boscolo Bariga Luigi	Consigliere	Confcommercio	Priv/parti econ. e soc.	X	
Melotti Claudio	Consigliere	Cassa Rurale Vallagarina	Priv/parti econ. e soc		X
Castellani Fabio	Consigliere	Confesercenti	Priv/parti econ. e soc	X	
Sandri Alberto	Consigliere	ANCE Verona	Priv/parti econ. e soc	X	

Presenti n. 7, Assenti n. 2

Assiste alla seduta e ne cura la verbalizzazione Il Segretario dott.ssa Elisabetta Brisighella

Il dr. Ermanno Anselmi, nella sua qualità di Presidente, assume la presidenza e, riconosciuta legale la seduta, la dichiara aperta.

REFERTO DI PUBBLICAZIONE ON LINE

Io sottoscritto Segretario, certifico che copia del presente verbale viene pubblicata oggi 06.07.2022 all'Albo dell'Associazione G.A.L. "Baldo-Lessinia"

Il Segretario

F.TO dott.ssa Elisabetta Brisighella

LETTO CONFERMATO E SOTTOSCRITTO		COPIA CONFORME ALL'ORIGINALE
Il Presidente F.TO dott. Ermanno Anselmi	Il Segretario F.TO dott.ssa Elisabetta Brisighella	Il Segretario dott.ssa Elisabetta Brisighella

IL CONSIGLIO DI AMMINISTRAZIONE

Premesso

- che con deliberazione n. 39 del 22.09.2021 il Consiglio di Amministrazione ha affidato l'incarico del servizio di assistenza in ambito "privacy" relativo allo svolgimento delle funzioni di Responsabile Della Protezione Dei Dati Personali - Data Protection Officer (DPO) per il GAL Baldo Lessinia all'Avv.to Paola Finetto;
- che si è provveduto a verificare e aggiornare tutti i documenti e applicazioni in ambito privacy in possesso del GAL;
- che è stato redatto un "Modello Privacy" per definire, nell'ambito della organizzazione aziendale ed operativa dell'Ente stesso, quanto segue:
    - i dati personali trattati (precisamente da dipendenti, collaboratori, consulenti) con riferimento a persone fisiche, nonché le modalità di trattamento;
    - le responsabilità e le modalità con cui gestire la protezione dei dati personali secondo i princìpi della *data protection by design and by default* (art. 25 Regolamento UE 679/2026), della responsabilizzazione (art. 5 co. 2 Regolamento UE 679/2026), oltre che sulla base dei princìpi di liceità correttezza e trasparenza (art. 5 co. 1.a Regolamento UE 679/2026), limitazione della finalità (art. 5 co. 1.b Regolamento UE 679/2026), minimizzazione dei dati (art. 5 co. 1.c Regolamento UE 679/2026), esattezza (art. 5 co. 1.d Regolamento UE 679/2026), limitazione della conservazione (art. 5 co. 1.e Regolamento UE 679/2026), integrità e riservatezza (art. 5 co. 1.f Regolamento UE 679/2026), comunque con riferimento alle norme applicabili ed in particolare a quelle del Regolamento e del Codice Privacy, tenendo peraltro conto anche dei provvedimenti e delle autorizzazioni resi dell'Autorità Garante per la Protezione dei Dati italiana (di seguito indicata come se e in quanto applicabili;
    - le procedure tecnico-organizzative e relative modalità di gestione adottate al fine di garantire un livello di sicurezza, per i dati personali in formato elettronico e cartaceo o con altri mezzi di trattamento, adeguato ai rischi in conformità all'art. 32 del Regolamento UE 679/2026;

Vista

- la revisione effettuata in ambito Privacy per il GAL Baldo-Lessinia con i relativi documenti che sono parte integrante di questo provvedimento (Allegato 1);

Ritenuto

- approvare la revisione e tutta la documentazione rielaborata in ambito Privacy per il GAL Baldo-Lessinia;

Visti

- il Regolamento (UE) N. 1303/2013 del Consiglio, del 17 dicembre 2013, definisce le norme comuni ai fondi SIE e il Regolamento (UE) N. 1305/2013 del Consiglio, del 17 dicembre 2013 definisce le norme applicabili al sostegno da parte del Fondo europeo agricolo per lo sviluppo rurale (FEASR);

- l’Accordo di Partenariato adottato dalla Commissione Europea in data 29 ottobre 2014 che definisce la strategia per un uso ottimale dei Fondi strutturali e di investimento europei in Italia per la programmazione 2014-2020;

- la DGR n. 947 del 28.07.2015 con cui è stato approvato il Programma di Sviluppo Rurale per il Veneto 2014-2020 (PSR), a seguito dell'approvazione della Commissione Europea avvenuta con decisione C(2015) 3482 del 26.05.2015 e sue successive modifiche ed integrazioni;

- la DGR n. 1214 del 15.09.2015 con cui la Regione Veneto ha approvato il bando di selezione per il finanziamento della Misura 19, relativa al Sostegno allo Sviluppo Locale LEADER-SLTP Sviluppo Locale di Tipo Partecipativo del PSR 2014-2020 e successive integrazioni alle disposizioni tecnico operative;

- la DGR n. 1937 del 23.12.2015 con cui la Regione Veneto ha approvato il documento "Indirizzi Procedurali Generali" del PSR 2014-2020, che è stato oggetto di successivi adeguamenti e integrazioni;

- la DGR n. 1547 del 10.10.2016 con cui sono stati approvati i Gruppi di Azione Locale e relativi Programmi di Sviluppo Locale, ai fini dell’attuazione del Programma di Sviluppo Rurale Leader 2014-2020, e al GAL “Baldo-Lessinia” è stato assegnato un contributo pubblico pari a 8.966.315,40 Euro;

- la Deliberazione n. 40 del 29.11.2016, con la quale il Consiglio di Amministrazione del GAL ha approvato il P.S.L. 2014-2020 “IN.S.I.E.M.&: Iniziativa a Sostegno delle Imprese e dell’Economia Montana del Baldo & Lessinia”;

- la deliberazione n. 41 del 26.07.2018 con cui il Consiglio di amministrazione del GAL Baldo-Lessinia ha approvato in via definitiva l’Atto Integrativo Speciale prendendo atto della comunicazione e delle prescrizioni ricevute con prot. 0288505 del 06.07.2018 da parte della 4irezione AdG FEASR Parchi e Foreste della Regione Veneto;

- la DGRV n. 1065 del 03.08.2021 con cui si è provveduto all’assegnazione, ai PSL selezionati con DGRV n. 1547/2016, delle risorse aggiuntive FEASR 2021/2022 e sono stati adeguati i termini e le scadenze per l’esecuzione dei TI 19.2.1, 19.3.1 e 19.4.1 approvando lo schema di “Atto Integrativo Regolamento (UE) 2020/2220”;

- la deliberazione n. 37 del 22.09.2021 con cui il Consiglio di Amministrazione del GAL ha approvato l’Atto Integrativo Regolamento (UE) 2020/2220” e lo “Schema 2 - Scheda riepilogativa Atti integrativi PSL” per l’allocazione delle risorse aggiuntive 2021-2022;

- la DDR n. 44 del 22.10.2021 con cui sono stati approvati gli esiti delle istruttorie svolte sugli Atti Integrativi Reg. 2020/2022 presentati dai GAL del Veneto e, in particolare, quello relativo al GAL Baldo-Lessinia fissa in euro 11.245.469,46 la dotazione finanziaria complessiva del PSL 2014-2022 e che le risorse complessive per il TI 19.2.1 sono di euro 9.754.108,85 e per il TI 19.4.1 sono di euro 1.491.360,61;

- Regolamento UE 679/2026 “Regolamento generale sulla protezione dei dati personali” e del D.Lgs.196/2003 “Codice in materia di protezione dei dati personali” come modificato, da ultimo, dal D.Lgs. 18/05/2018 n. 51 e dal D.Lgs. 10/08/2018 n. 101;

Richiamata

- l’attenzione dei presenti sull’obbligo del rispetto del principio di non conflitto d‘interessi, con riferimento all’oggetto della deliberazione da adottare e acquisita la dichiarazione degli stessi sull’insussistenza di conflitto d’interessi in merito alla deliberazione in oggetto, come previsto dalla deliberazione n. 23 assunta dal Consiglio di Amministrazione del GAL nella seduta del 26.05.2021;

Rilevata

- l'insussistenza di situazioni di conflitto di interesse da parte dei consiglieri, sulla base delle dichiarazioni rilasciate dagli stessi, in merito alla presente deliberazione;

Accertato

- che almeno il 50% dei Consiglieri presenti rappresenta le parti economiche e sociali e la società civile come disposto dall'Art.34 del Reg. UE 1303/2013;

Con voti favorevoli e unanimi, resi secondo quanto previsto dall'art. 37 co 5 del Reg. CE 1974/2006, così come modificato dal Reg. di esecuzione (UE) 679/2011 della Commissione europea,

D E L I B E R A

1. **Di approvare** le premesse che costituiscono parte integrante e sostanziale del presente provvedimento.
2. **Di approvare** la documentazione in ambito Privacy redatta per il GAL Baldo-Lesssinia che allegata al presente atto ne costituisce parte integrante (Allegato 1).
3. **Di confermare** che la presente deliberazione è stata adottata nel rispetto degli obblighi previsti dalla DGR 1214/2015, in particolare a garanzia che almeno il 50% dei voti espressi nelle decisioni di selezione provenga da partner che non sono autorità pubbliche.
4. **Di confermare** che la presente deliberazione è stata adottata nel rispetto degli obblighi previsti dalla DGR 1214/2015 in particolare in materia di conflitto di interessi e trasparenza dei processi decisionali.
5. **Di disporre** la pubblicazione nella pagina Amministrazione Trasparente del sito web dell'Associazione www.baldolessinia.it.

Così deliberato in data 13 giugno 2022

Il Presidente	Il Segretario
F.TO dott. Ermanno Anselmi	F.TO dott.ssa Elisabetta Brisighella

Allegato 1

GAL Baldo Lessinia

Via Giulio Camuzzoni 8 – 37038 Soave (VR)
C.F. 93102010233
www.baldolessinia.it

MODELLO PRIVACY

(Regolamento UE n. 679/2016)
(D.Lgs. 196/2003 e ss.mm.)

Approvazione e adozione del Modello Privacy	Aggiornamento del Modello Privacy	Data

INDICE

Premessa.

Il presente documento viene redatto dal **Gruppo di Azione Locale** (**GAL) Baldo Lessinia** con sede legale in 37038 Soave (VR), Via Giulio Camuzzoni 8, codice fiscale 93102010233, in persona del presidente, e-mail: gal@baldolessinia.it, PEC: baldolessinia@pec.net, quale Titolare del trattamento (di seguito indicata anche come "**Ente**"), in conformità a quanto previsto dalla normativa nazionale vigente in materia di protezione dei dati personali delle persone fisiche e, in particolare, in conformità alle disposizioni del Regolamento UE 679/2016 "Regolamento generale sulla protezione dei dati" (di seguito indicato come "**Regolamento**") e del D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato, da ultimo, dal D.Lgs. 18/05/2018 n. 51 e dal D.Lgs. 10/08/2018 n. 101 (di seguito indicato come "**Codice Privacy**").

Il GAL Baldo Lessinia è un'Associazione composta attualmente da 53 soci, di cui 35 Comuni, 2 Comunità Montane, 1 consorzio e 15 privati fra cui associazioni, banche, strade, consorzi e associazioni di categoria. Il GAL pubblica bandi di finanziamento della Misura 19 del PSR della Regione Veneto, destinati sia a soggetti pubblici che a privati. Le richieste vengono finanziate a seguito di valutazioni effettuate da AVEPA (l'organismo della Regione Veneto dedicato a questa attività per tutti i finanziamenti e contributi) in collaborazione con il GAL. Tutti i bandi vengono pubblicati sul sito www.baldolessinia.it e pubblicizzati attraverso i social. Dal confronto fra i rappresentanti locali nascono le progettualità cosiddette di "tipo partecipativo". Il GAL gestisce lo sviluppo locale di tipo partecipativo nelle zone rurali come voluto dall'Unione Europea che lo definisce "Sviluppo Locale Leader". Leader è la sintesi di "Liaison entre Actions de Développement de l'Economie Rurale" – Collegamento tra azioni di sviluppo dell'economia rurale). Nell'attuale periodo di programmazione dei fondi UE (2014-2020), Leader rappresenta proprio la

sopracitata Misura 19 “Sostegno allo sviluppo locale – Leader” contenuta all’interno del PSR e del FEASR regionale.
La progettazione partecipativa del GAL è realizzata attraverso una strategia di sviluppo locale con obiettivi e risultati definiti all’inizio di ogni programmazione europea che ha una durata di 7 anni. L’attuale Programma di Sviluppo Locale del GAL Baldo Lessinia 2014-2020 è denominato IN.S.I.E.M.& e ha una dotazione finanziaria complessiva di 8.966.336,90 euro. Questi fondi, al netto di quelli impegnati per la gestione dell’organizzazione del GAL (Misura 19.4.1), sono destinati ai bandi per le imprese e per la Pubblica Amministrazione.

(1)
Obiettivi e ambito di applicazione; principi normativi.

Scopo del Modello Privacy adottato dall’Ente e presentato in questo documento è definire, nell’ambito della organizzazione aziendale ed operativa dell’Ente stesso:

- i dati personali [i] trattati (precisamente da dipendenti, collaboratori, consulenti) con riferimento a persone fisiche, nonché le modalità di trattamento [ii] ;
- le responsabilità e le modalità con cui gestire la protezione dei dati personali secondo i princìpi della *data protection by design and by default* (art. 25 Regolamento [iii]), della responsabilizzazione (art. 5 co. 2 Regolamento [iv]), oltre che sulla base dei princìpi di liceità correttezza e trasparenza (art. 5 co. 1.a Regolamento [v]), limitazione della finalità (art. 5 co. 1.b Regolamento [vi]), minimizzazione dei dati (art. 5 co. 1.c Regolamento [vii]), esattezza (art. 5 co. 1.d Regolamento [viii]), limitazione della conservazione (art. 5 co. 1.e Regolamento [ix]), integrità e riservatezza (art. 5 co. 1.f Regolamento [x]), comunque con riferimento alle norme applicabili ed in particolare a quelle del Regolamento e del Codice Privacy, tenendo peraltro conto anche dei provvedimenti e delle autorizzazioni resi dell’Autorità Garante per la Protezione dei Dati italiana [xi] (di seguito indicata come “**Garante Privacy**”) se e in quanto applicabili; a tali fonti normative si farà di seguito riferimento come “**Norme Applicabili**”;
- le procedure tecnico-organizzative e relative modalità di gestione al fine di garantire un livello di sicurezza per i dati personali in formato elettronico e cartaceo o con altri mezzi di trattamento adeguato ai rischi in conformità all’art. 32 del Regolamento.

L’Ente si prefigge di operare nel pieno rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, con specifico riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati, comunque assicurando l’applicazione dei princìpi sopra enunciati sulla base di un'attenta valutazione sostanziale e non formalistica delle garanzie previste, nonché di un'analisi della quantità e qualità delle informazioni utilizzate e dei possibili rischi connessi al relativo trattamento, al fine di prevenire ed evitare qualsivoglia violazione dei dati personali [xii].

Per una più immediata e sintetica esposizione e comprensione dai trattamenti effettuati, dei dati trattati e delle finalità di trattamento, nonché delle banche dati [xiii] nella disponibilità dell’Ente, si rinvia ai registri delle attività di trattamento – **allegati 1A e 1B**.

(2)
Organizzazione e ripartizione dei compiti e delle responsabilità

in ambito aziendale.

Ai fini di una corretta e completa gestione della privacy con riferimento alle Norme Applicabili ed ai princìpi richiamati nel paragrafo precedente, l'Ente ha provveduto alla individuazione dei soggetti di seguito indicati.

2.1) Titolare del trattamento (art. 24 Regolamento) [xiv]:

Titolare del trattamento è il **Gruppo di Azione Locale** (**GAL) Baldo Lessinia** con sede legale in 37038 Soave (VR), Via Giulio Camuzzoni 8, codice fiscale 93102010233, in persona del presidente, e-mail: gal@baldolessinia.it, PEC: baldolessinia@pec.net.

Per i fini di cui alle Norme Applicabili e in conformità alle medesime, il Titolare provvede a definire una gerarchia di responsabilità e competenze in relazione alla protezione dei dati personali, individuando tra i dipendenti o tra i consulenti dell'Ente, soggetti capaci ed affidabili a cui delegare, in tutto o in parte, la gestione (applicazione, verifica, implementazione) delle procedure aziendali sulla privacy, previste e richiamate nel presente documento. Al riguardo si rinvia all'Organigramma di cui all'**allegato 1C**.

In relazione alle specifiche attività svolte dall'Ente, non ricorre l'ipotesi di contitolarità del trattamento (art. 26 Regolamento), essendo l'Ente e i singoli Associati, di cui all'**allegato 2**, titolari autonomi dei trattamenti di dati di cui alle rispettive aree di competenza.

Infine, poiché il Titolare è stabilito nell'Unione Europea, non è necessario procedere alla nomina di un rappresentante del titolare nell'Unione e non trova applicazione l'art. 27 Regolamento.

2.2) Responsabili del trattamento (art. 28 Regolamento) [xv]:

Laddove l'Ente affidi il trattamento dei dati personali, in tutto o in parte, a soggetti terzi, questi ultimi effettueranno il trattamento per conto dell'Ente nella propria qualità di Titolare. In questo caso l'Ente dovrà nominare il terzo quale Responsabile del trattamento, a tal fine avvalendosi di un accordo scritto il cui contenuto includa quanto previsto dall'art. 28 Regolamento.

Il Titolare dovrà preventivamente verificare che il nominando Responsabile presenti garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate, affinché il trattamento effettuato per conto del Titolare stesso soddisfi i requisiti previsti dalle Norme Applicabili e garantisca la piena tutela dei diritti degli interessati.

Per la nomina dei Responsabili del trattamento si dovrà utilizzare il documento "Nomina del Responsabile del trattamento" – **allegato 3.**

2.2.1) Amministratore di sistema [xvi]:

Una figura particolare di Responsabile del trattamento è l'Amministratore di sistema, per tale intendendosi la persona fisica nominata ai sensi del provvedimento del Garante Privacy del 27/11/2008, così come successivamente modificato, con particolare riferimento al provvedimento del 29/06/2009.

L'Amministratore di sistema (per brevità AdS) sovrintende alle risorse del sistema operativo e al buon funzionamento dell'infrastruttura informatica aziendale. Laddove il Regolamento prevede un nucleo minimo di misure che rispondono a criteri di sicurezza predefiniti (art. 25 Regolamento), in particolare:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

la nomina di un Amministratore di sistema costituisce una ulteriore procedura e misura idonea a garantire che il Modello Privacy adottato dall'Ente sia conforme alle Norme Applicabili [xvii].

L'attribuzione delle funzioni di AdS deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dati, ivi compreso il profilo relativo alla sicurezza. La nomina deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, tra i quali:

- predisporre il sistema per il cambio delle password almeno ogni tre mesi;
- predisporre le misure necessarie per evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up;
- assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- fare in modo che sia prevista la disattivazione dei codici identificativi personali (USER-ID) in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure in caso di mancato utilizzo dei codici identificativi personali (USER-ID) per oltre sei mesi;
- proteggere il sistema informatico dal rischio d'intrusione (violazione del sistema da parte di "hacker") e dal rischio di virus utilizzando i sistemi di volta in volta tecnologicamente più aggiornati;

attenendosi comunque scrupolosamente alle prescrizioni del Garante Privacy contenute nei provvedimenti del 27/11/2008, così come successivamente modificato, con particolare riferimento al provvedimento del 29/06/2009, alle Norme Applicabili e alle istruzioni dell'Ente.

Per la nomina dell'AdS si dovrà utilizzare il documento "Nomina dell'Amministratore di sistema" – **allegato 4**.

2.3) Incaricati del trattamento (art. 29 Regolamento) [xviii]:

Gli Incaricati del trattamento (anche detti preposti al trattamento o autorizzati al trattamento) sono persone fisiche autorizzate al trattamento dei dati dal Titolare o dal Responsabile e sotto la responsabilità di questi ultimi.

Gli Incaricati vengono nominati con riferimento a trattamenti specifici, con particolari responsabilità e mansioni, ciascuno nell'ambito delle specifiche istruzioni ricevute e dell'area di responsabilità e competenza loro attribuita dal Titolare o dal Responsabile.

Gli Incaricati hanno il compito di:

- operare nel rispetto del Modello Privacy, di cui al presente documento, comunque sulla base delle istruzioni ricevute dal Titolare o Responsabile;
- confrontarsi con il Titolare o il Responsabile o il DPO, se nominato, in merito a qualsiasi dubbio circa la concreta applicazione del presente Modello Privacy;
- informare senza indugio il Titolare o il Responsabile e comunque il DPO, se nominato, sulle non corrispondenze con il Modello Privacy in generale e, immediatamente, in caso di violazioni dei dati personali;
- cooperare con il Titolare o il Responsabile e il DPO, se nominato, per qualsiasi attività diretta a promuovere la conoscenza e la formazione relativamente al presente Modello Privacy;
- svolgere le attività previste dai trattamenti rientranti nella dichiarazione di nomina, attenendosi scrupolosamente alle prescrizioni contenute nel presente documento, nelle istruzioni ricevute dal Titolare/Responsabile e nelle direttive del DPO, se nominato;
- astenersi dal modificare i trattamenti esistenti e dall'introdurre nuovi trattamenti senza l'esplicita autorizzazione scritta del Titolare/Responsabile o del DPO, se nominato;
- informare immediatamente il Titolare/Responsabile e comunque il DPO, se nominato, in caso di richieste da parte degli interessati di esercitare i diritti previsti dalle Norme Applicabili.

Per la nomina degli Incaricati del trattamento si dovrà utilizzare il documento "Nomina dell'Incaricato del trattamento" – **allegato 5**.

2.4) Responsabile della protezione dei dati (RPD/DPO) (artt. 37-38-39 Regolamento) [xix]:

L'Ente, per l'attività in concreto svolta, ritiene di dover provvedere alla nomina di un RPD/DPO, tenuto conto di quanto previsto dall'art. 37 Regolamento, oltre che dalle Linee Guida del WP Art. 29 del 13/12/2016 modificate il 05/04/2017 "*Guidelines on Data Protection Officers*" [xx].

Ai fini della nomina del RPD/DPO, l'Ente stesso dovrà attenersi alle indicazioni seguenti.

Il RPD/DPO è un soggetto (persona fisica o persona giuridica) designato dal Titolare, con apposito accordo scritto (dichiarazione di nomina se persona fisica; contratto di servizi se persona giuridica), per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento. Il RPD/DPO deve cooperare con il Garante Privacy e, proprio per questo, il suo nominativo dev'essere comunicato al Garante Privacy. Il RPD/DPO costituisce inoltre il punto di contatto e di riferimento rispetto agli interessati, per le questioni connesse al trattamento dei dati personali e per l'esercizio dei diritti loro attribuiti dalle Norme Applicabili. Il RPD/ DPO è designato e nominato dall'Ente sulla base e tenendo conto delle sue competenze e qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, della capacità di assolvere i compiti di cui agli artt. 38 e 39 Regolamento. Nello specifico il RPD/DPO è tenuto a:

- informare e fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalle Norme Applicabili;
- sorvegliare l'osservanza delle Norme Applicabili nonché delle politiche dell'Ente in materia di protezione dei dati personali come indicate nel presente documento e nei suoi allegati nonché negli altri documenti comunicati ai dipendenti e collaboratori dell'Ente, ivi comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 Regolamento;
- cooperare con il Garante Privacy;
- fungere da punto di contatto per il Garante Privacy per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- promuovere lo svolgimento di un continuo programma di formazione degli Incaricati del trattamento;
- se del caso promuovere l'aggiornamento del Modello Privacy aziendale, di cui al presente documento;
- se necessario, conservare e monitorare l'aggiornamento del Registro delle Attività del Trattamento di cui all'art. 30 Regolamento;
- verificare e monitorare la correttezza dei documenti costituenti il presente Modello Privacy e di quelli successivamente resi sulla base dello stesso

Per la nomina del RPD/DPO si dovrà utilizzare il documento "Nomina del Responsabile della protezione dei dati – RPD/DPO" – **allegato 6**.

(3)
Identificazione dei dati e dei trattamenti

Il presente Modello Privacy si applica nell'ambito della gestione del trattamento di dati personali afferenti persone fisiche e riguarda:

- le attività di trattamento di dati ed informazioni di carattere personale, cioè riferite direttamente o indirettamente ad una persona fisica, effettuate da o per conto del Titolare, ovunque venga effettuato il trattamento stesso;
- le attività svolte dal Titolare dirette ad approntare e implementare le misure tecniche ed organizzative adeguate a garantire che il trattamento è effettuato conformemente alle Norme Applicabili;
- le attività dirette a consentire e rendere effettivo l'esercizio dei diritti attribuiti agli interessati dalle Norme Applicabili e, dunque, a titolo meramente esemplificativo, il diritto di informazione e accesso ai propri dati personali, il diritto alla rettifica ed alla cancellazione ("diritto all'oblio"), il diritto alla limitazione del trattamento, alla portabilità dei dati e, ove previsto dal Regolamento, all'opposizione al trattamento;
- le attività di comunicazione e diffusione di dati personali ed eventuale trasferimento di dati personali all'estero;
- ogni altra forma di trattamento di dati personali prevista dalle Norme Applicabili.

I dati trattati dal Titolare, come di seguito analiticamente specificati, sono forniti da utenti, partner e fornitori di beni e/o servizi, nonché da dipendenti e collaboratori, ai fini della erogazione dei servizi richiesti e dell'adempimento degli obblighi di legge.

Si tratta di dati personali [xxi], inclusi i dati sensibili [xxii] (per tali intendendosi i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale e quelli attinenti alla salute fisica o mentale di una persona fisica), nonché i dati giudiziari [xxiii] , che l'Ente tratta in occasione o nell'ambito delle attività svolte per fini di inserimento, accesso ed elaborazione, modifica, annullamento, comunicazione a terzi per finalità specifiche, con strumenti elettronici e non elettronici. Al riguardo si rinvia ai registri delle attività di trattamento – **allegati 1A e 1B**.

(4)
Analisi dei rischi che incombono sui dati trattati.

L'Ente si riserva di effettuare una **valutazione d'impatto sulla protezione dai dati** in conformità all'art. 35 Regolamento, in particolare a fronte dell'eventuale utilizzo di nuove tecnologie e, nel caso in cui, considerati la natura, l'oggetto, il contesto e la finalità del trattamento, questo possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. A questo riguardo all'Ente è noto che, come peraltro già comunicato dal Garante Privacy, la CNIL (Autorità francese per la protezione dei dati) ha messo a disposizione un software di ausilio ai titolari in vista della effettuazione della precitata valutazione d'impatto. Il software offre un percorso guidato alla realizzazione della valutazione d'impatto secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla valutazione d'impatto medesima. La versione di questo software in lingua italiana è stata messa a punto con la collaborazione del Garante Privacy ed è gratuitamente disponibile sul sito web del Garante Privacy. Ai fini di una futura valutazione d'impatto, dunque, l'Ente potrà avvalersi di tale software, pur ricordando che esso è in continua evoluzione.

Al momento, considerata l'attività svolta dall'Ente e valutati i possibili rischi nell'ambito della gestione del trattamento dei dati personali, il Titolare ritiene di poter adottare le misure di sicurezza specificate nel paragrafo che segue, al fine di garantire la minimizzazione di tali rischi e prevenire eventuali violazioni nel trattamento dei dati, oltre che per poter dimostrare, all'occorrenza, le concrete iniziative tecnico-organizzative assunte dall'Ente in conformità alle Norme Applicabili (principio della responsabilizzazione).

(5)
Misure adottate per garantire i dati e i trattamenti.

Per quanto concerne le misure tecnico-organizzative in concreto adottate dall'Ente [xxiv] per prevenire i rischi di cui sopra e, comunque, per ridurne quanto più possibile l'impatto, con riferimento anche alla identificazione delle risorse hardware e software, nonché di rete di cui si avvale l'Ente per trattare i dati oggetto del presente Modello Privacy, di cui all'**allegato 7**, si evidenzia quanto segue.

Le banche dati trattate mediante supporti non elettronici (= cartacei) vengono conservate in archivi chiusi a chiave o in apposite stanze dotate di serratura oltre che in apposite casseforti. Le chiavi di accesso ai singoli

archivi sono custodite dal Titolare, dal Responsabile, se nominato, e dagli Incaricati del trattamento all'uopo nominati. Per le banche dati trattate mediante supporti elettronici vengono utilizzati personal computer o server con accesso tramite dispositivo elettronico di sicurezza e dotati di programma antintrusione e antivirus; l'accesso contemporaneo con una stessa User-ID non è consentito e i supporti non utilizzati vengono cancellati. Ai fini di una più dettagliata e completa esplicitazione delle misure tecnico-organizzative attuate dall'Ente per la gestione di tali archivi, elettronici e non elettronici, con riferimento ai dati personali trattati, al fine di eliminare o comunque minimizzare i rischi di violazione dei dati, si rinvia ai regolamenti relativi all'uso dei pc e delle risorse informatiche – **allegati 8A e 8B**.

La bontà delle misure adottate è periodicamente verificata come per legge a cura dell'Ente, il quale, a tal fine, si avvarrà di consulenti e tecnici esterni e dunque esenti da conflitti d'interesse.

Inoltre, l'Ente e i soggetti dal medesimo Incaricati del trattamento dei dati ovvero nominati quali Responsabili del trattamento dei dati si impegnano e devono impegnarsi a garantire che i dati personali degli interessati siano:

- trattati in modo lecito, corretto e trasparente;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (c.d. minimizzazione dei dati);
- esatti e, se necessario, aggiornati, peraltro impegnandosi l'Ente ad assicurare che siano adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principi della integrità e riservatezza).

A tal fine i predetti soggetti dovranno operare in conformità alle concrete istruzioni e misure tecnico-organizzative indicate dall'Amministratore di Sistema, se nominato, o dal Titolare, per quanto riguarda:

- ✓ gestione e utilizzo di beni e risorse informatiche, servizi ICT e reti informative;
- ✓ gestione e utilizzo account;
- ✓ gestione e utilizzo credenziali di autenticazione/password;
- ✓ gestione postazioni di lavoro
- ✓ utilizzo di personal computer e computer portatili;
- ✓ gestione e utilizzo software;
- ✓ gestione e utilizzo di dispositivi mobili di connessione (internet key);
- ✓ gestione e utilizzo di dispositivi di memoria portatili;
- ✓ gestione e utilizzo di stampanti, fotocopiatrici e fax;
- ✓ gestione e utilizzo di strumenti di fonia mobile e/o di connettività in mobilità;
- ✓ gestione e utilizzo della rete intranet aziendale;
- ✓ gestione e utilizzo della rete internet;
- ✓ gestione e utilizzo della posta elettronica aziendale - accesso alla casella di posta elettronica del lavoratore assente - cessazione dell'indirizzo di posta elettronica aziendale;

- ✓ protezione antivirus;
- ✓ regole comportamentali per la prevenzione di attacchi informatici.

Premessi i princìpi generali di comportamento, di cui sopra, si rinvia ai regolamenti relativi all'uso dei pc e delle risorse informatiche – **allegati 8A e 8B**.

Inoltre, e più in generale, premesso che l'Ente non trasferisce dati personali all'estero, né all'interno dell'Unione Europea né verso paesi terzi, valgono e si applicano le regole di sicurezza di seguito specificate, con la precisazione che le presenti istruzioni si applicano a tutti i lavoratori dipendenti e a tutti i collaboratori del Titolare, a prescindere dal rapporto contrattuale con lo stesso intrattenuto (lavoratori somministrati, collaboratori a progetto, agenti, stagisti, consulenti, ecc.), i quali si trovano ad operare sui dati personali di cui l'Ente stesso è Titolare ovvero Responsabile per conto dei terzi Titolari (di seguito "utenti"):

- al momento della raccolta dai dati (se raccolti presso l'interessato) ovvero entro massimo 30 giorni dalla raccolta dei dati (se raccolti da terzi o inviati spontaneamente dall'interessato) dev'essere consegnata all'interessato un'apposita informativa, utilizzando il modello predisposto dall'Ente – **allegati 9 e 9bis**; l'informativa sottoscritta dall'interessato dev'essere prontamente trasmessa o consegnata all'Ente in originale;
- al momento della raccolta dai dati (se raccolti presso l'interessato) ovvero entro massimo 30 giorni dalla raccolta dei dati (se raccolti da terzi o inviati spontaneamente dall'interessato) e, comunque, in ogni caso di trattamento di dati sensibili, giudiziari o che richiedono una particolare attenzione, così come in caso di trattamento per plurime finalità, dev'essere acquisito il consenso [xxv] dell'interessato, utilizzando il modello predisposto dall'Ente – **allegato 10**; il modulo di raccolta del consenso sottoscritto dall'interessato dev'essere prontamente trasmesso o consegnato all'Ente in originale;
- provvedere tempestivamente, alla rettifica, modificazione, cancellazione dei dati raccolti ogni qual volta l'interessato lo richieda per iscritto e comunque, quanto alla cancellazione, ogni qual volta i dati raccolti non siano più necessari per le finalità del trattamento o se la loro ulteriore conservazione non è più lecita né legittima, in ogni caso dandone comunicazione all'interessato.

Si precisa tuttavia che, per quanto le misure di sicurezza adottate siano idonee a ridurre notevolmente gli eventuali episodi di danno o pericolo per i dati oggetto di trattamento, non può escludersi a priori che si possano verificare eventi eccezionali di distruzione o danneggiamento. Per evitare che eventi di tal fatta si traducano nella perdita definitiva ed irrecuperabile dei dati stessi, tali informazioni sono protette: dall'uso di password e di nomi utenti; da backup con cui si provvede a fare copia dei dati trattati elettronicamente e il relativo supporto mobile è custodito in luogo sicuro protetto e provvisto di impianto antincendio; sono inoltre presenti misure di sicurezza per i luoghi fisici di cui si è già riferito. Anche a questo riguardo, si rinvia alle concrete misure tecniche indicate dal nominando Amministratore di Rete e/o di Sistema e, comunque, a quanto previsto nei regolamenti relativi all'uso dei pc e delle risorse informatiche – **allegati 8A e 8B**.

Nel caso in cui, nonostante le misure di sicurezza adottate, si verifichi una **violazione di dati personali nell'ambito delle operazioni di trattamento effettuate dall'Ente (*data breach*)**, il Regolamento prevede che il Titolare debba notificare la violazione all'autorità di controllo competente e, quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche,

anche all'interessato senza ingiustificato ritardo. Tra i possibili incidenti, che possono causare violazioni dei dati personali, si ricordano a titolo esemplificativo:

- *perdita o furto di strumenti IT (pc, smartphone, chiavette USB, hardware);*
- *rivelazione di informazioni a soggetti non autorizzati;*
- *accesso non autorizzato ai dati personali;*
- *violazione delle misure di sicurezza fisiche dei locali dove i dati personali sono archiviati;*
- *caricamento/divulgazione per errore di dati personali in rete;*
- *errore umano (per esempio: perdita di dati personali archiviati presso luoghi non sicuri);*
- *mancata previsione di eventi di rischio per la sicurezza dei dati quali allagamenti o incendi;*
- *attacco esterno ai sistemi IT aziendali;*
- *reati informatici.*

Ebbene, laddove si verifichi una tale violazione, dovrà essere seguita la **procedura** di seguito descritta, al fine di assicurare una gestione controllata, strutturata ed efficace degli incidenti e prevenire il verificarsi di altre violazioni:

a) scoperta o sospetta violazione dei dati: il soggetto, che viene a conoscenza di una violazione di dati personali, anche solo sospetta e non ancora accertata, deve informare immediatamente il proprio superiore gerarchico o il Titolare; quest'ultimo deve a sua volta immediatamente riferire al RDP/DPO (se nominato);

b) relazione interna sulla violazione dei dati: il Titolare o il superiore gerarchico o soggetti da questi delegati devono quanto prima, possibilmente entro 24 ore dalla notizia dell'evento, redigere una relazione interna sull'occorso, specificando data e ora, soggetti coinvolti, descrizione dell'incidente, dati personali apparentemente violati, sistemi/reti/archivi interessati, iniziative eventualmente già assunte per mitigare le conseguenze dell'incidente;

c) valutazione del rischio per i diritti e le libertà delle persone: il Titolare o il superiore gerarchico o soggetti da questi delegati, sulla base delle circostanze concrete della violazione verificatasi o sospettata e del potenziale rischio per i diritti e le libertà degli interessati, dovranno individuare tempestivamente i soggetti, interni o esterni alla Società, dotati delle necessarie competenze al fine di eseguire le verifiche e/o le investigazioni relative alla violazione dei dati e valutare gli eventuali danni provocati dalla stessa, tenendo in considerazione e sulla base del tipo di violazione, della natura, della gravità, del volume di dati personali, della facilità di identificazione degli interessati, delle caratteristiche particolari degli interessati o del Titolare, oltre che del numero di persone interessate coinvolte (attenzione: si deve ritenere che la violazione dei dati abbia comportato un rischio per i diritti e le libertà delle persone fisiche, laddove la violazione possa causare danni materiali o immateriali alle persone fisiche, tra cui a titolo esemplificativo perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata); tali verifiche dovranno essere concluse, ove possibile, entro 24 ore dal momento del loro avvio;

   - ✓ se la valutazione si conclude con esito negativo e, dunque, risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare o il soggetto da questo delegato ne darà atto nella relazione interna, annoterà

l'incidente nel registro delle violazioni a tale scopo approntato (**allegato 11**), riferirà al RDP/DPO (se nominato);

- ✓ se la valutazione si conclude con esito positivo e, dunque, risulti probabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare o il soggetto da questi delegato dovrà, comunque entro 72 ore dall'incidente, notificare l'avvenuta violazione al Garante Privacy tramite l'apposita procedura disponibile online; dovrà altresì darne atto nella relazione interna, annotare l'evento nel registro delle violazioni all'uopo approntato (**allegato 11**), riferire al RDP/DPO (se nominato), comunque darne comunicazione all'interessato; in ogni caso ci si dovrà attenere a quanto prescritto dagli artt. 33 e 34 del Regolamento.

(6)
Trattamenti specifici.

Al momento l'Ente non effettua trattamenti specifici (ad esempio, videosorveglianza, geolocalizzazione), che necessitino di una specifica regolamentazione.

(7)
Formazione.

Per rendere gli Incaricati del trattamento edotti dei rischi che incombono sui dati trattati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto all'attività svolta dall'Ente, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dall'Ente, vengono organizzati periodicamente (a cadenza annuale) programmi di formazione tecnica e teorica.

Sono tenuti a seguire i programmi di formazione tutti i dipendenti e i collaboratori che, a vario titolo, sono chiamati ad operazioni di trattamento dei dati dal momento della loro assunzione e sempre in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento stesso.

Obiettivo della formazione curata dall'Ente, in ragione della peculiare attività svolta, è anche quello di sensibilizzare gli Incaricati a prestare particolare attenzione all'adozione di idonee cautele per prevenire l'ingiustificata raccolta, utilizzazione o conoscenza di dati, anche in caso di:

- acquisizione anche informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possono comportare, comunque, rischi specifici per gli interessati;
- scambio di corrispondenza, specie per via telematica;
- utilizzo di dati di cui è dubbio l'impiego lecito, anche per effetto del ricorso a tecniche invasive;
- utilizzo e distruzione di dati riportati su particolari dispositivi o supporti, specie elettronici (ivi comprese registrazioni audio/video), o documenti;
- custodia di materiale documentato, ma non utilizzato in un procedimento e ricerche su banche dati a uso interno, specie se consultabili anche telematicamente da uffici dello stesso titolare del trattamento situati altrove;
- acquisizione di dati e documenti da terzi, verificando che si abbia titolo per ottenerli;
- conservazione di atti relativi ad affari definiti.

Gli Incaricati vengono formati anche sull'obbligo di non attuare prassi elusive di obblighi e di limiti di legge e, in particolare, di conformarsi ai princìpi fondamentali enunciati dalle Norme Applicabili.

Le attività formative svolte ed i relativi destinatari e partecipanti vengono documentate e la relativa documentazione è conservata nella sede dell'Ente.

(8)
Implementazione del Modello Privacy.

All'insorgere di nuove attività aziendali, quali nuovi servizi erogati o dipartimenti costituiti, l'Ente, anche a mezzo di personale preposto, dovrà darne tempestiva notizia al RDP/DPO, se nominato. Dovrà inoltre provvedere a tutte le valutazioni e le attività necessarie in conformità al presente Modello Privacy e alle Norme Applicabili.

Il presente Modello e le relative procedure sono sottoposti ad *audit* interno su base semestrale da parte del RDP/DPO per l'individuazione di eventuali non conformità e per la valutazione delle relative azioni correttive. Ove il RDP/DPO non fosse stato nominato, l'Ente incaricherà un consulente esterno per la effettuazione di un *audit* specifico con cadenza annuale.

(9)
Allegati.

Si allegano al presente documento:

1.A – Registro attività di trattamento
1.B – Registro categorie attività di trattamenti
1.C – Organigramma GDPR
2 – Elenco Associati
3 – Nomina responsabile del trattamento
4 – Nomina amministratore di sistema
5 – Nomina incaricato del trattamento
6 – Nomina RPD/DPO
7 – Diagramma network
8.A – Regolamento pc
8.B – Regolamento strumenti informatici
9 – Informativa
9bis – Informativa selezione personale
10 – Raccolta del consenso
11 – Registro delle violazioni

[i] Per “dato personale” si intende, a norma dell’art. 4.1 Regolamento, *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*.

[ii] Per “trattamento” si intende, a norma dell’art. 4.2 Regolamento, *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*.

[iii] Il principio *privacy by design* implica l’obbligo per il titolare di configurare il trattamento prevedendo fin dall’inizio le garanzie indispensabili in conformità al Regolamento per tutelare i diritti dell’interessato, tenendo conto dello specifico contesto in cui avviene il trattamento e dei rischi che il trattamento può comportare. Il principio *privacy by default* comporta che la Società (e gli enti in generale) per impostazione predefinita tratti solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il tempo strettamente necessario secondo tali finalità; il sistema privacy adottato deve dunque soddisfare anche questo requisito.

[iv] Il principio di *accountability* (o responsabilizzazione) tende ad assicurare una effettiva garanzia dell'interessato in un'ottica di massima trasparenza. Al titolare del trattamento è affidato l'incarico di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati; a sua volta, il titolare deve essere in grado di dimostrare di avere adottato misure tecnico-organizzative adeguate ed efficaci per la protezione dei dati personali.

[v] I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

[vi] I dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.

[vii] I dati personali trattati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono stati raccolti e sono quindi oggetto di trattamento.

[viii] I dati personali trattati devono essere 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 stati raccolti e sono oggetto di trattamento.

[ix] I dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati raccolti e sono trattati.

[x] I dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza degli stessi, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

[xi] Autorità di controllo per l’Italia ai sensi dell’art. 51 Regolamento.

[xii] *Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati* (art. 4.12 Regolamento). Il considerando (85) del Regolamento richiama l’attenzione su tali violazioni, precisando che *una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata*.

[xiii] Q*ualsiasi 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* (art. 4 n. 6 Regolamento).

[xiv] *1. 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, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l’attuazione di*

politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

[xv] L'art. 28 Regolamento stabilisce, tra l'altro, che i *trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico (...) che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.*

[xvi] Il Garante Privacy, con provvedimento del 27/11/2008 e ss.mm., ha precisato che, in assenza di definizioni normative e tecniche condivise, ai fini privacy l'amministratore di sistema è assunto quale figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (*enterprise resource planning*), le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

[xvii] Del resto, il considerando (49) del Regolamento stabilisce che *costituisce legittimo interesse del titolare del trattamento (...) trattare dati personali (...) in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.*

[xviii] Il Regolamento, pur non prevedendo espressamente la figura autonoma dell'incaricato del trattamento di cui all'abrogato art. 30 D.Lgs. 196/2003, fa comunque riferimento a persone autorizzate al trattamento dei dati personali sotto l'autorità del Titolare o del Responsabile (art. 29).

[xix] Art. 37 Regolamento: *1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;* ***b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;*** *oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10. 2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento. 3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. 4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento. 5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39. 6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. 7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.*

[xx] Il Garante Privacy ha al riguardo concluso nel senso che *sono tenuti alla nomina, a titolo esemplificativo e non esaustivo:* (…) *società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); (...) società che forniscono servizi informatici (...)*.

[xxi] Q*ualsiasi informazione riguardante una persona fisica identificata o identificabile; 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 (art. 4 n. 1 Regolamento).*

[xxii] Il considerando (10) del Regolamento fa riferimento al *trattamento di categorie particolari di dati personali («dati sensibili»)*. La nozione generale di dati particolari o sensibili è offerta dall'art. 9 co. 1 del Regolamento, articolo rubricato "*Trattamento di categorie particolari di dati personali*", ove tali dati sono qualificati come *dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché (...) 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*.
Il considerando (51) del Regolamento specifica che *meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i* ***dati personali che rivelano l'origine razziale o etnica*** e, altresì, precisa che le **fotografie** rientrano nell'ambito dei dati sensibili, nello specifico dei *dati biometrici*, soltanto quando esse sono trattate *attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica*.
La nozione di **dati biometrici** è ripresa nell'art. 4 n. 14 del Regolamento; essi sono qualificati come *dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*.
Ancora, il considerando (34) si riferisce espressamente ai ***dati genetici*** qualificandoli come *dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti*. L'art. 4 n. 13 del Regolamento ne ribadisce la definizione, precisando che dati genetici sono i *dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione*.
Il considerando (35) individua poi i ***dati personali relativi alla salute*** e specifica che tali sono *tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione (...) un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.* L'art. 4 n. 15 del Regolamento ribadisce che i dati relativi alla salute sono *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*.

[xxiii] Il Regolamento, nel considerando (91) e nell'art. 10 fa riferimento a *dati relativi a condanne penali e reati o a connesse misure di sicurezza*.

[xxiv] L'art. 32 Regolamento, rubricato "sicurezza del trattamento", stabilisce:
1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo

richieda il diritto dell'Unione o degli Stati membri.

[xxv] La regola generale prevista dalle Norme Applicabili è che è sempre necessario il consenso espresso e specifico dell'interessato. Nei seguenti casi, tra gli altri, non è tuttavia necessario acquisire preventivamente il consenso dell'interessato:

- per l'esecuzione di un contratto del quale l'interessato è parte;
- per l'adempimento di un obbligo di legge cui è soggetto il Titolare;

laddove il trattamento sia necessario per il perseguimento del legittimo interesse del Titolare.