DOCUMENTO ORGANIZZATIVO PRIVACY
E
REGISTRO DEI TRATTAMENTI

Redatto ai sensi dell'art. 30 del Regolamento Generale sulla Protezione dei Dati (GDPR) 2016/679

Titolare del trattamento:
ISTITUTO COMPRENSIVO "ISOLE EOLIE"

Via Stradale snc – 98055 Lipari (ME) – C.F. 81001350834

Tel. +39 090 9812222 – Mail: meic818009@istruzione.it

Dirigente Scolastica pro-tempore: **dott.ssa Mirella Fanti**

Data Protection Officer:

Indo S.r.l.s.

Sede Legale: Viale G. Mancini 156 Cosenza (CS) – P. IVA 03510180783

Tel. +39 02 87366082 – e.mail: dpo@indoconsulting.it

nominato in data 01/10/2021 Prot:0007351.01/10/2021

mail di contatto: dpo@indoconsulting.it

Revisione:	*3*
Data revisione:	*21/11/2023*
Motivo della revisione	*Aggiornamento soggetti autorizzati*

INDICE

1. SCOPO DEL DOCUMENTO ORGANIZZATIVO PRIVACY E DEL REGISTRO DEI TRATTAMENTI

Il presente documento rappresenta la revisione, alla data indicata, del Documento Organizzativo Privacy dell' **Istituto Comprensivo "Isole Eolie"** del Comune di Lipari (ME), predisposto in modo da rispondere alle disposizioni del D.Lgs 196/2003 coordinato con le disposizioni del D.Lgs 101/2018 entrato in vigore il 19 settembre 2018 e del Regolamento Europeo sulla protezione dei dati REG. EU 679/2017 entrato in vigore il 25 maggio 2018.

Con il presente documento il Titolare del trattamento dei dati ottempera altresì agli obblighi previsti dall'art. 30 del Regolamento sul Trattamento di Dati che prevede la redazione del **Registro dei Trattamenti** in qualità di **Titolare del trattamento.**
Il registro dei trattamenti ai sensi dell'art. 30 è un documento contenente le principali informazioni relative alle operazioni di trattamento svolte, obbligatorio per i seguenti soggetti:

- imprese o organizzazioni con almeno 250 dipendenti;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti che possano presentare un rischio – anche non elevato – per i diritti e le libertà dell'interessato;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti delle categorie particolari di dati di cui all'articolo 9, paragrafo 1 RGPD, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 RGPD.

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

2.1 Titolare del trattamento

Alla data del presente documento si è proceduto ad analizzare nuovamente l'organigramma per la gestione della protezione dei dati, implementato al momento dell'entrata in vigore della nuova normativa, e, ove necessario ad aggiornarlo.

Il GDPR 679/2016 individua le seguenti figure.
Il **Titolare** è, secondo l'articolo 4 del suddetto regolamento, 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; nello specifico è l' **Istituto Comprensivo " Isole Eolie " nella persona del Dirigente Scolastico dott.ssa Mirella Fanti.**

In ossequio alla nota del Garante per la protezione dei dati personali del 27 febbraio 2019 ed in virtù del D. Lgs 9 aprile 2008 n.81 contente la disciplina in materia di igiene e sicurezza sul luogo di lavoro, l'**Istituto Comprensivo " Isole Eolie"** si avvale della **dott.ssa Tringali Maria Antonietta** per lo svolgimento delle attività di trattamento dei dati correlate alla figura di medico del lavoro e sorveglianza sanitaria, la stessa agisce in qualità di Titolare autonomo del trattamento.

2.2 Responsabile della protezione dati (RPD/DPO)

L'adeguamento e l'implementazione del livello di protezione dei dati personali è in continuo aggiornamento.

Con l'entrata in vigore del Reg. UE 2016/679, nel maggio 2018, l'**Istituto Comprensivo "Isole Eolie"** è tenuto alla designazione obbligatoria del RPD nei termini previsti, rientrando nella fattispecie prevista dall'art. 37, par. 1, lett b) e c) del RGPD.

Dopo attenta valutazione delle proprie risorse interne e ricerca di mercato ha ritenuto che la Società **Indo S.r.l.s.,** sia in possesso del livello di conoscenza specialistica e delle competenze richieste dall'art. 37, par. 5, del RGPD, per la nomina a RPD, e non si trova in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare.

Per questo motivo, l' **Istituto Comprensivo " Isole Eolie "** ha designato la società **Indo S.r.l.s.** avente sede legale in Viale Mancini n. 156 – cap. 87100 Cosenza – ITALIA C.F/P.IVA 03510180783, nella persona della dott.ssa Michela Simonetti quale Responsabile della protezione dei dati personali (RPD).

All'interno della **Indo S.r.l.s.** è presente un'organizzazione idonea a guidare e verificare la protezione dei dati personali all'interno della struttura.

2.3 Responsabili esterni del trattamento per conto del Titolare

Il Titolare ha nominato diversi Responsabili del trattamento, secondo l'art. 28 del GDPR 2016/679, ciascuno per le competenze del proprio settore.

Sono Responsabili esterni tutti i soggetti esterni all'Istituto che effettuano trattamenti sulle banche dati dello stesso, per suo conto e nel suo interesse; qualora, invece, questi determini autonomamente le finalità ed i mezzi del trattamento, deve considerarsi titolare dei trattamenti in questione.

I trattamenti da parte del Responsabile del trattamento sono disciplinati, ai sensi dell'art. 28 GDPR, da un contratto o altro atto giuridico che individui la durata, la natura, la finalità del trattamento, il tipo di dati personali e le categorie degli interessati, le responsabilità affidate al Responsabile, gli obblighi ed i diritti del Titolare.

Il Responsabile esterno del trattamento tiene, al pari del Titolare, il registro delle attività di trattamento di cui all'art. 30 n. 2 GDPR, svolte per conto del Titolare stesso.

Il Responsabile del trattamento non può trattare i dati personali se non secondo le istruzioni impartite dal Titolare ed in caso di trattamenti particolarmente complessi può nominare, a sua volta, un sub-responsabile.

Di seguito i soggetti individuati:

NOME RESPONSABILE	*ATTIVITA' SVOLTA*	*NOME REFERENTE*	*CONTATTO*
Argo Software Srl	*servizi di assistenza e aggiornamento registro elettronico, segreteria digitale, software di contabilità e cloud server*		*Sede legale:* *Zona Industriale III Fase* *Viale 24 N. 7* *97100 Ragusa* *C.F.- P.I va e R.I. di RG* *00838520880* *Tel. 0932.666412* *Mail:* *info@argosoft.it*
We Plus Srls	*Servizi di manutenzione ed* *assistenza tecnica, assistenza su software, servizi in cloud e manutenzione e assistenza impianto di videosorveglianza*		*Sede legale:* *Via Comunale Zafferia Coop.* *''Rosa Lavina'' scala D* *98127 Messina (ME)* *P.IVA: 03588330831* *Mail:* *amministrazione@weplus.it*
Ing. Catalano Domenico Studio di Ingegneria	*servizi di prevenzione e protezione in qualità di R.S.P.P. ai sensi della L: 81/08*		*Sede legale:* *S.S. 106 III TR. TV. H, 37/B* *89134 Reggio Calabria* *Tel. +39 392 7248430* *C.F. CTLDNC76R01H224D* *Mail:* *catalanodomenico@hotmail.it*

2.4 Amministratore di sistema

In ossequio al Provvedimento a carattere generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relative alle attribuzioni delle funzioni di amministratore di sistema" il Titolare del trattamento non ha nominato nessun Amministratore di Sistema. Gli eventuali problemi tecnici, sia hardware che software, sugli elaboratori vengono risolti da società esterne dietro chiamata a necessità

2.5 Soggetti autorizzati al trattamento interni alla realtà scolastica

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto ad **unità organizzativa** o **singolo incaricato** di trattamento. Le responsabilità sono dettagliate per iscritto nella lettera di nomina (allegato 1). L'elenco delle banche dati inserito nelle lettere di nomina registra la situazione alla data della firma delle stesse.

Attualmente sono **autorizzati** al trattamento dei Dati Personali le seguenti **unità organizzative**:

Unità Organizzativa **Personale Docente e assimilati**
Unità Organizzativa **Collaboratori Scolastici**
Unità Organizzativa **Personale Area Amministrativa**

Direttore servizi generali amministrativi **"Dsga", dott.ssa Susanna Rando.**

Ed inoltre:

Assistente Tecnico Informatico
Riccardo Napoli

Animatore Digitale
Agata Finocchiaro

3. TIPOLOGIE DEI DATI TRATTATI

A seguito dell'analisi compiuta si sono identificati i seguenti trattamenti:

- Dati **comuni** relativi al **personale**, necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria, nonché di natura **particolare** conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o l'adesione ad organizzazioni sindacali;
- Dati **comuni** relativi a **fornitori** dagli stessi forniti, indispensabili allo svolgimento dei rapporti contrattuali, compresi i dati sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
- Dati **comuni, particolari** e **giudiziari** relativi agli alunni frequentanti necessari per le finalità istituzionali dell'Istituto che sono quelle dell'istruzione e formazione degli alunni nonché quelle amministrative ad esse strumentali così come definite dalla normativa statale e regionale;
- Dati **comuni**, **particolari e giudiziari** relativi agli **ex alunni** necessari per le finalità istituzionali dell'Istituto così come previsto dalla normativa statale e regionale;
- Dati **comuni** dei **genitori degli alunni** o gli **esercenti la patria potestà** per le notizie che trasmettono, per la partecipazione agli organi collegiali come previsto dal regolamento interno e dalla normativa statale e regionale.

3.1 Integrazione cessazione emergenza COVID.19 - 2023/2024

In considerazione della cessazione del periodo emergenziale sono venute meno le misure previste per il contenimento dello stesso, l'Istituto pertanto ha aggiornato il proprio sistema di gestione privacy facendo decadere le nomine predisposte per il trattamento dati finalizzato alla gestione dei dati legate al contenimento del Covid 19.

4. FINALITA' DI TRATTAMENTO E COMUNICAZIONE DEI DATI

I dati oggetto di trattamento rientrano nelle finalità per le quali il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, obblighi legali di cui è investito il titolare del trattamento ai sensi dell'art. 6 lettera e) del Regolamento UE 2016/679.

La comunicazione dei dati a eventuali persone fisiche e/o Autorità pubbliche, avverrà nell'ambito del perimetro previsto da normative nazionali e comunitarie e/o da leggi e regolamenti regionali.

5. REGISTRO DEI TRATTAMENTI

Si riportano di seguito, in dettaglio, le attività di trattamento svolte all'interno della struttura del Titolare:

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Alunni Genitori	**RACCOLTA NOMINATIVI ALUNNI E GENITORI**	Elenchi iscrizione, ammissione, frequenza trasferimento	Segreteria Area alunni Area didattica	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☑Giudiziari	Argo Software Srl	U.O. Docenti e assimilati U.O. Personale amministrativo	Fornita in sede di richiesta di iscrizione	Richiesto consenso ai sensi dell'art 7 GDPR 679/2016	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni	**TENUTA REGISTRI E STRUMENTI DI VALUTAZIONE ALUNNI**	Valutazione Alunni	Segreteria Area Alunni	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari	Argo Software Srl	U.O. Docenti e assimilati	Fornita in sede di iscrizione	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Alunni	**DIETE REFEZIONE SCOLASTICA**	Richiesta di pasti personalizzati per motivi di salute ed etnico religiosi	Segreteria Area Didattica	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Docenti e assimilati U.O. Collaboratori scolastici U.O. Personale amministrativo	Fornita in sede di iscrizione	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni	**CONCESSIONE BUONO LIBRO**	Libri di testo	Segreteria Area Alunni	☑ Comuni ☐ Genetici ☐ Biometrici ☑Particolari ☐ Giudiziari		U.O. Personale amministrativo	Come da trattamento alunni	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Alunni	**SCHEDA DELLE COMPETENZE**	Gestione e archiviazione documentazione essenziale prodotta dagli alunni durante il percorso formativo	Area didattica Segreteria	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Docenti e assimilati	Fornita in sede di iscrizione	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni	**RACCOLTA NOMINATIVI PARTECIPANTI A VIAGGI D'ISTRUZIONE COMPRESE** **IMMAGINI E FOTO**	Organizzazione viaggi d'istruzione	Area didattica Segreteria	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Docenti e assimilati U.O. Personale amministrativo	Come da trattamento alunni	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni, Enti e Istituzioni	**RAPPORTI CON ASL E ENTI LOCALI**	Tenuta dei rapporti con enti ed istituzioni al fine di favorire l'inserimento degli alunni nel tessuto sociale	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑Particolari ☐ Giudiziari		U.O. Docenti e assimilati U.O. Personale amministrativo	Come da trattamento alunni	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Insegnanti alunni	**PROGETTI ELABORATI DAGLI INSEGNANTI**	Tenuta sintesi dei progetto elaborati D.lgs 297/94	Segreteria Area didattica	☑ Comuni ☐ Genetici ☐ Biometrici ☐ Particolari ☐ Giudiziari		U.O. Docenti e assimilati U.O. Personale amministrativo	Come da trattamento alunni	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni	**CONSULTAZIONE FASCICOLO PERSONALE ALUNNO**	Fascicolo personale alunno	Segreteria Area didattica	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Docenti e assimilati	Come da trattamento alunni	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni Dipendenti	**CIRCOLARI INTERNE**	Redazione circolari interne e comunicazione ai destinatari	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☐ Particolari ☐ Giudiziari		U.O. Personale amministrativo	Come da trattamento Alunni e dipendenti	Come da trattamento alunni e dipendenti	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Dipendenti	**FASCICOLI PERSONALI DIPENDENTI**	Tenuta fascicoli personali, certificati di servizio, pratiche nuovi assunti e pensioni	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☑Giudiziari		Dsga Susanna Rando U.O. Docenti e assimilati U.O. Personale amministrativo	Fornita in sede di inizio rapporto di lavoro	Esonero ai sensi dell'art. 9 GDPR 679/2016	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Alunni Dipendenti	**ATTIVITA' CONNESSE ALLA MANUTENZIONE DEL SISTEMA E DEI DISPOSITIVI INFORMATICI IN USO AL FINE DEL MANTENIMENTO DELLE FUNZIONALITA' DELLA STRUMENTAZIONE INFORMATICA E A SUPPORTO DELLA GESTIONE DELLA DIDATTICA NELL'UTILIZZO DELLE PIATTAFORME DIGITALI, COMPRESA L'EVENTUALE CONFIGURAZIONE**	Gestione funzionalità strumentazione informatica e supposto gestione didattica piattaforme digitali	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		Riccardo Napoli	Come da trattamento alunni e dipendenti	Come da trattamento alunni e dipendenti	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Dipendenti	**FASCICOLO DIPENDENTI**	Liquidazioni trattamento economico al personale dip.; Attribuzione agevolazioni fiscali retributive (assegni fam.); Trattenimento sullo stipendio per iscrizioni ai sindacati, scioperi, ecc; Relazioni periodiche agli Enti assicurativi, assistenziali, previdenziali; Rilascio certific. dei redditi; Compilazioni ruoli per fisco ed enti assicurativi, assistenziali e previdenziali; Elaborazioni statistiche (conto annuale). Obbligo previsto dal DLgs 135/99, TU 165/2001	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☑Giudiziari		Dsga Susanna Rando U.O. Personale amministrativo	Fornita in sede di inizio rapporto di lavoro	Esonero ai sensi dell'art. 9 GDPR 679/2016	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Alunni Dipendenti	**COORDINARE LA DIFFUSIONE DELL'INNOVAZIONE DIGITALE NELL'AMBITO DELLE AZIONI PREVISTE DAL PTOF, PIANO TRIENNALE DELL'OFFERTA FORMATIVA E LE ATTIVITA' DEL PNSD, PIANO NAZIONALE SCUOLA DIGITALE (NELLO SPECIFICO FORMAZIONE INTERNA, COINVOLGIMENTO DELLA COMUNITA' SCOLASTICA E CREAZIONE SOLUZIONI INNOVATIVE)**	Gestione attività PNSD	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		Agata Finocchiaro	Come da trattamento alunni e dipendenti	Come da trattamento alunni e dipendenti	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Elettori attivi e passivi	**ELEZIONI ORGANI COLLEGIALI**	Formazione degli elenchi degli elettori divisi per categoria. Istituzione di commissioni elettorali Costituzione dei seggi Formazione delle liste. Predisposizione dei vari tipi di schede. Svolgimento dello scrutinio. Proclamazione degli eletti. . D.Lgs. 297/94 (T.U. Sulla Scuola) L.27/10/95 n.437	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☑Giudiziari		U.O. Docenti e assimilati U.O. Personale amministrativo	Come da trattamento elettori	Come da trattamento elettori	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni	**RACCOLTA DATI NECESSARI ALLA VALUTAZIONE E ORIENTAMENTO SCRUTINI DE ESAMI**	Valutazione e scrutini ed esami	Segreteria Area Didattica	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Docenti e Assimilati	Come da trattamento alunni	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Alunni	**RACCOLTA DEI DATI NECESSARI AD EVENTUALI RECLAMI, RICORSI O CONTENZIOSO CON ALUNNI**	Rapporti scuola-famiglia Gestione contenzioso	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Docenti e Assimilati	Come da trattamento alunni	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni Fornitori Dipendenti	**CONTABILITA'**	Tenuta rapporti con i fornitori Redazione Bilancio consuntivo Attività negoziale – investimenti D.lgs297/94 – L. 59/97 D.M. 93/99	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		Dsga Susanna Rando	Come da trattamento fornitori e dipendenti	Come da trattamento fornitori e dipendenti	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni Dipendenti fornitori	**PROTOCOLLO**	Archiviazione posta in entrata ed in uscita. Archiviazione comunicazioni varie	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Personale amministrativo	Come da trattamento Alunni fornitori e dipendenti	Come da trattamento Alunni fornitori e dipendenti	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Alunni	**RACCOLTA E CONSULTAZIONE DEI DATI RELATIVI ALL'ACCOGLIENZA E ALLA SORVEGLIANZA DEGLI ALUNNI**	Sorveglianza e accoglienza alunni	Segreteria Are didattica	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Collaboratori scolastici	Come da trattamento Alunni	Come da trattamento Alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni	**GESTIONE DEI DATI RELATIVI AGLI ALUNNI PER L'AUSILIO AI PORTATORI DI HANDICAP**	Supporto alunni con disabilità	Segreteria Area didattica	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Collaboratori scolastici	Come da trattamento Alunni	Come da trattamento Alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Alunni	**RACCOLTA E CONSULTAZIONE DEI DATI RELATIVI ALLA COLLABORAZIONE CON IL CORPO DOCENTE**	Gestione del rapporto di collaborazione per lo svolgimento delle attività didattiche	Segreteria Area didattica	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Collaboratori scolastici	Come da trattamento Alunni	Come da trattamento Alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

CATEGORIA DI INTERESSATI	TRATTAMENTO	FINALITA'	UFFICIO DI RIFERIMENTO	NATURA DEI DATI	RESPONSABILE DEL TRATTAMENTO	SOGGETTI AUTORIZZATI/ UNITA' ORGANIZZATIVE	INFORMATIVA	CONSENSO	TEMPO DI CONSERVAZIONE DEI DATI	TRASFERIMENTO DATI
Dipendenti	**GESTIONE GRADUATORIE INSEGNANTI. ARCHIVIAZIONE E TITOLI**	Graduatorie insegnanti Graduatorie Personale ATA	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Personale amministrativo	Come da trattamento dipendenti	Come da trattamento dipendenti	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Dipendenti	**ASSICURAZIONI INFORTUNI**	Pratiche di assicurazione per ogni alunno, tenuta registri infortuni L. 626/94 D.lgs 297/94 (T.U. sulla Scuola)	Segreteria Area Alunni	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari		U.O. Personale amministrativo	Come da trattamento alunni	Come da trattamento alunni	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE
Dipendenti	**ARCHIVIO L. 81/2008**	Gestione di problematiche particolari scaturenti dall'applicazione della L. 81/2008 Obbligo previsto dalla L. 81/2008	Segreteria Area amministrativa	☑ Comuni ☐ Genetici ☐ Biometrici ☑ Particolari ☐ Giudiziari			Come da trattamento dipendenti	Come da trattamento dipendenti	Come normativa di riferimento	☑ Non previsto ☐ Paesi UE ☐ Paesi Extra UE

6. MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Il trattamento dei dati avviene negli uffici di segreteria collocati nella sede centrale di Via Stradale snc- 98055 Lipari (ME). Gli uffici di segreteria si trovano al primo piano di un edificio protetto da un sistema di allarme e di video sorveglianza. Tutti gli ambienti sono dotati di estintori ed armadi ignifughi.

Gli archivi cartacei si trovano c/o la sede centrale di Lipari in una stanza archivio.

L'accesso del Personale ATA viene controllato da un registro ingressi.

Il trattamento avviene con le seguenti modalità:

A – Schedari ed altri supporti cartacei

I supporti cartacei vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo, in appositi armadi siti nei locali della segreteria, nell'ufficio del DSGA e del Dirigente Scolastico ai quali accedono solo le persone autorizzate

B – Struttura informatica – Segreteria digitale.

Gli uffici di segreteria dispongono di n. 7 PC utilizzati con sistema operativo Windows 10 e identificati in rete con indirizzo dinamico DHCP. I PC sono protetti all'accesso da password e da antivirus Windows Defender e firewall su software Microsoft. Sui PC vengono eseguite copie di sicurezza sia su Raid che su NAS e custodite all'interno della sede in un armadio chiuso a chiave. L'Istituto dispone anche di un server HP Proliant -Windows 2019, collocato in un armadio rack con porte di accesso monitorate, sistema di condizionamento, gruppo di continuità e sistema di videosorveglianza interno. Giornalmente e su NAS vengono eseguite copie di sicurezza del server utilizzato e custodite all'interno della sede in un armadio chiuso a chiave. Inoltre, viene anche utilizzata una rete WI FI con password robuste ed efficaci.

C. Registro elettronico

Secondo quanto previsto dall'art.7, commi 27 e 31 del d.l. 6 luglio 2012, n.95, convertito con modificazioni in legge 7 agosto 2012 n.135, a decorrere dall'anno scolastico 2012-2013 le istituzioni scolastiche e i docenti adottano registri *on line* e inviano le comunicazioni agli alunni e alle famiglie in formato elettronico.

L'Istituto utilizza il Registro Elettronico fornito dalla società **ARGO SOFTWARE SRL** individuato come Responsabile del trattamento ai sensi dell'art.28 del GDPR. Per le modalità operative, le procedure di abilitazione e i profili di autorizzazione attribuiti alle diverse categorie di utenti sono individuati nella documentazione specifica rilasciata dal fornitore del servizio.

D – Impianti di video-sorveglianza

Sulla sede principale di Lipari è presente un impianto di videosorveglianza, al momento, in verifica e revisione.

7. ANALISI DEI RISCHI E MISURE ADOTTATE

COMPONENTI DEL RISCHIO

L'analisi dei possibili rischi che gravano sui dati è stata effettuata combinando due tipi di rilevazione:

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- le caratteristiche degli strumenti utilizzati per il trattamento dei dati.

Si stima il grado di rischio, che dipende dalla **tipologia dei dati trattati dal Titolare**, combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono:

GRADO DI INTERESSE PER I TERZI					
	ELEVATISSIMO				
	ALTO	**1.** Dati comuni alunni e genitori		**2.** Dati particolari e/o giudiziari degli alunni	
	MEDIO			**3.** Dati particolari personale	
	BASSO	**4.** Dati comuni di fornitori e terzi			
		BASSO	**MEDIO**	**ALTO**	**ELEVATISSIMO**

PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO

Si nota che un grado di rischio alto, o addirittura elevatissimo, è collegato al trattamento dei seguenti dati, alla tutela dei quali devono quindi essere dedicate particolari attenzioni:

- quelli idonei a rivelare informazioni di carattere particolare o giudiziario dei soggetti interessati o del personale, che sono accomunati dall'aspetto critico di avere un elevato grado di pericolosità per la privacy dei soggetti interessati;
- quelli che costituiscono una importante risorsa, per il Titolare, in relazione ai danni che conseguirebbero da una eventuale perdita, o trafugamento, dei dati.

Per quanto concerne gli strumenti impiegati per il trattamento, le componenti di rischio possono essere idealmente suddivise in

1. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:
   - al verificarsi di eventi distruttivi (incendi, allagamenti, corti circuiti)
   - alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici)

2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti)

3. rischio di penetrazione logica nelle reti di comunicazione

4. rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti

Alla luce dei fattori di rischio e delle aree individuate precedentemente, vengono descritte le misure atte a garantire:

- la **protezione delle aree e dei locali** ove si svolge il trattamento dei dati personali
- la **corretta archiviazione e custodia** di atti, documenti e supporti contenenti dati personali
- la **sicurezza logica**, nell'ambito degli strumenti elettronici

Le successive misure indicate a sostegno della fase di protezione dei dati si suddividono in

- misure già adottate al momento della stesura del presente documento
- ulteriori misure finalizzate ad incrementare il livello di sicurezza nel trattamento dei dati

LA PROTEZIONE DI AREE E LOCALI

Per quanto concerne il rischio che incombe sui locali ove si svolge il trattamento dei dati, sono previste le seguenti misure di sicurezza.

Rischio
Accessi non autorizzati agli uffici ad accesso ristretto **Impatto sulla sicurezza:** Accesso ai dati da parte di soggetti non autorizzati e/o accesso ai dati per trattamenti non consentiti
Misure adottate
Portone accesso rinforzato
Sistemi di allarme e di videosorveglianza antintrusione – sede principale Lipari

Rischio
Accessi dei dipendenti fuori l'orario di lavoro **Impatto sulla sicurezza** Accesso ai dati da parte di soggetti in orari non consentiti
Misure adottate
Autorizzazione del Dirigente Scolastico
Chiusura dei locali

Rischio
Asporto materiale cartaceo destinato allo smaltimento rifiuti **Impatto sulla sicurezza** Accesso ai dati da parte di soggetti non autorizzati
Misure adottate
Istruzione agli incaricati
Riporre i documenti negli appositi sacchi di plastica, assicurare una chiusura ermetica degli stessi ed asportarli giornalmente

Rischio
Errori umani nella gestione della sicurezza fisica **Impatto sulla sicurezza** Accesso ai dati da parte di soggetti non autorizzati e/o accesso ai dati per trattamenti non consentiti

Misure adottate
Portone accesso rinforzato
Sistemi di allarme e di videosorveglianza antintrusione – sede principale Lipari

Rischio
Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria **Impatto sulla sicurezza** Distruzione totale o parziale dei dati e/o inibizione dell'accesso ai dati
Misure adottate
Predisporre piano di Disaster Recovery
Estintori
Copie di sicurezza dei dati adeguate

Rischio
Guasto ai sistemi complementari **Impatto sulla sicurezza** Distruzione totale o parziale dei dati e/o inibizione dell'accesso ai dati
Misure adottate
Sistemi UPS che garantiscono la continuità elettrica

Rischio
Sottrazione di strumenti contenenti dati **Impatto sulla sicurezza** Distruzione totale o parziale dei dati e/o diffusione non autorizzata di dati
Misure adottate
Sistemi di allarme e di videosorveglianza antintrusione – sede principale Lipari
Portone di accesso rinforzato

CUSTODIA E ARCHIVIAZIONE DEI DATI

Agli incaricati sono state impartite istruzioni per la gestione, la custodia e l'archiviazione dei documenti e dei supporti, e sono state previste idonee misure di sicurezza.

Rischio
Accesso non autorizzato **Impatto sulla sicurezza** Accesso ai dati per trattamenti non consentiti
Misure adottate

Assegnazione, ad uso esclusivo, di una o più credenziali di autenticazione agli operatori
Assegnazione di parole chiave che rispondono ai requisiti di sicurezza e che sono modificate ciclicamente
Disattivazione delle credenziali di autenticazione in caso di perdita di qualità dell'incarico
Individuazione del profilo di autorizzazione anteriormente all'inizio del trattamento
Aggiornamento periodico o al verificarsi di eventuali modifiche della lista degli incaricati e dei profili di autorizzazione
Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durante le sessioni di lavoro
Istruzioni in merito all'accesso agli archivi

Rischio Carenza di consapevolezza, disattenzione, incuria o indisponibilità **Impatto sulla sicurezza** Comportamenti contrari ai principi di sicurezza e protezione dei dati
Misure adottate
Formazione sugli aspetti principali del Regolamento Europeo al momento dell'ingresso in servizio
Formazione, periodica e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti per il trattamento dei dati e la loro protezione
Istruzioni finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento senza l'ausilio di strumenti elettronici
Adozione di procedure per le copie di sicurezza, la loro custodia ed il ripristino della disponibilità dei dati
Individuazione dei soggetti incaricati alla custodia delle copie delle credenziali
Procedure di verifica sull'operato degli incaricati

Rischio Comportamenti sleali o fraudolenti **Impatto sulla sicurezza** Accesso ai dati per trattamenti non consentiti e/o contrari ai principi di sicurezza e protezione dei dati
Misure adottate
Definizione di responsabilità e sanzioni disciplinari
Controllo degli accessi ai dati e programmi
Monitoraggio continuo delle sessioni di lavoro

Rischio Errore materiale **Impatto sulla sicurezza** Operazioni accidentali non consentite e/o contrarie ai principi di sicurezza e protezione dei dati
Misure adottate

Formazione professionale
Reinstallazione dei programmi danneggiati o distrutti
Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati
Definizione delle procedure di convalida delle operazioni a rischio nell'ambito dell'incarico assegnato

Rischio Sottrazione di credenziali di autenticazione **Impatto sulla sicurezza** Accesso ai dati da parte di soggetti non autorizzati e/o accesso ai dati per trattamenti non consentiti
Misure adottate
Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione
Aggiornamento periodico delle credenziali di autenticazione

MISURE LOGICHE DI SICUREZZA

Per il trattamento effettuato con strumenti elettronici si sono individuate le seguenti misure:

- realizzazione e gestione di un **sistema di autenticazione informatica** al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici
- autorizzazione e definizione delle **tipologie di dati ai quali gli incaricati possono accedere** e utilizzare al fine delle proprie mansioni lavorative
- **protezione di strumenti e dati** da malfunzionamenti e attacchi informatici
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei **supporti rimovibili**, contenenti dati personali

SISTEMA DI AUTENTICAZIONE INFORMATICA

Il **sistema di autenticazione informatica** viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare, fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali;
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

L'eccezione vale, ovviamente, solo per gli strumenti elettronici che non siano in rete, o che siano in rete esclusivamente con strumenti elettronici non contenenti dati personali, o contenenti solo dati personali destinati alla diffusione.

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle **credenziali di autenticazione** per accedere ad un determinato strumento elettronico.

Per **realizzare** le credenziali di autenticazione si utilizza il seguente metodo:

- si associa un codice per l'identificazione dell'incaricato (*username)*, attribuito da chi amministra il sistema, ad una parola chiave riservata (*password*), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente.

Per l'**attribuzione e la gestione delle credenziali per l'autenticazione** si utilizzano i seguenti criteri:

- ad ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale;
- è invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- dovere di **custodire i dispositivi**, attribuiti agli incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici (ad esempio, il tesserino magnetico o la smart card): la custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici, che in quella in cui l'incaricato provveda a portare il dispositivo con sé (viene prescritto l'obbligo di custodirlo diligentemente). In ipotesi di smarrimento, l'incaricato deve provvedere immediatamente a segnalare la circostanza al Titolare del trattamento o all'Amministratore di Sistema, o alle altre persone che sono state a tale fine indicate, al momento dell'attribuzione del dispositivo
- obbligo di **non lasciare incustodito e accessibile lo strumento elettronico**, durante una sessione di trattamento, neppure in ipotesi di breve assenza
  - dovere di **elaborare in modo appropriato la password**, e di **conservare la segretezza** sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username). Agli incaricati è imposto l'obbligo di provvedere a modificare la password ciclicamente.

  Le **password** sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

  Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:

  - esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, ….)

  La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare). Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

  - scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata
  - consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password

  Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

TIPOLOGIE DI DATI AI QUALI GLI INCARICATI POSSONO ACCEDERE

Per quanto concerne le **tipologie di dati ai quali gli incaricati possono accedere**, ed i trattamenti che possono effettuare, si osserva che per gli incaricati sono previsti profili di autorizzazione distinti, in virtù del fatto che ciascuno può avere un accesso ai dati differenziato in base alla mansione ricoperta.

Le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e, se designato, dal responsabile, ovvero da soggetti da questi appositamente incaricati.

I profili di autorizzazione sono stati impostati sia per classi omogenee di incaricati (ad esempio, attribuendo un determinato profilo di autorizzazione a tutti gli impiegati di uno specifico settore) sia per singolo profilo di autorizzazione. L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun incaricato o di

ciascuna classe omogenea di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le mansioni lavorative.

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

PROTEZIONE DI STRUMENTI E DATI

Per quanto riguarda la **protezione di strumenti e dati**, da malfunzionamenti, attacchi informatici e programmi che contengono virus e malware, vengono adottate le misure descritte nello specifico allegato.

In generale Il primo aspetto affrontato riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).

Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine.

Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

SUPPORTI RIMOVIBILI

Per quanto concerne i **supporti rimovibili** (es. HD esterno, CD/DVD, chiavette USB….), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati particolari o giudiziari.

L'organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Per il trattamento effettuato con strumenti elettronici, dunque, si sono individuate le seguenti misure:

Rischio Accessi esterni non autorizzati **Impatto sulla sicurezza** Accesso agli strumenti per operazioni non consentite / non autorizzate
Misure adottate
Presenza di un sistema di autenticazione delle credenziali per tutti gli accessi agli archivi elettronici
Attivazione di uno screensaver automatico dopo pochi minuti di non utilizzo, con inserimento password per la prosecuzione del lavoro
Disattivazione delle credenziali di autenticazione nel caso di inutilizzo perdurato
Distruzione di tutti i supporti removibili non utilizzati

Utilizzo di un sistema Firewall sugli elaboratori

Rischio
Azione di virus informatici o di programmi suscettibili di recare danno **Impatto sulla sicurezza** Distruzione totale o parziale e/o diffusione non autorizzata e/o inibizione dell'accesso ai dati
Misure adottate
Utilizzo di un sistema antivirus
Aggiornamento periodico dei programmi antivirus
Aggiornamento periodico dei programmi per elaboratore contro la vulnerabilità dei dati

Rischio
Intercettazione di informazioni in rete **Impatto sulla sicurezza** Diffusione non autorizzata di dati
Misure adottate
Sistema di protezione dei dati trasmessi: predisposizione di Crittografia e Cifratura
Controlli periodici sul sistema di protezione nella trasmissione dei dati

Rischio
Malfunzionamento, guasti, eventi naturali, alterazioni delle trasmissioni, indisponibilità o degrado degli strumenti **Impatto sulla sicurezza** Distruzione totale o parziale dei dati e/o inibizione dell'accesso ai dati
Misure adottate
Manutenzione programmata degli strumenti
Controllo sull'operato degli addetti alla manutenzione
Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati
Istruzioni organizzative e tecniche per la custodia dei supporti removibili su cui sono memorizzati i dati
Sistemi UPS che garantiscono la continuità elettrica

Rischio
Spamming o tecniche di sabotaggio **Impatto sulla sicurezza** Distruzione totale o parziale e/o diffusione non autorizzata e/o inibizione dell'accesso ai dati

Misure adottate
Utilizzo di un sistema Firewall sugli elaboratori
Aggiornamento periodico del sistema Firewall
Controllo degli accessi a siti internet non sicuri
Divieto di scaricare software e di installare programmi da siti poco attendibili o non ufficiali
Disposizione di tenere sempre attiva l'opzione del browser "**richiedi conferma**" per l'installazione e il download di oggetti sulla propria macchina
Protezione della posta elettronica con disposizione di verifica della provenienza delle e-mail e di non esecuzione dei file allegati ai messaggi senza preventiva scansione antivirus
Utilizzo della casella di posta elettronica dell'ufficio come strumento di lavoro e dunque esclusivamente per esigenze lavorative

8. ALLEGATO N.1 - FAC – SIMILE LETTERA DI NOMINA SOGGETTO AUTORIZZATO

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI

AI SENSI DELL'ART. 2 QUATERDECIES DEL D.LGS 196/2003 NOVELLATO DAL D.LGS 101/2018

MANSIONI ED ISTRUZIONI

L' istituto **……** in qualità di Titolare del trattamento, visto l'art. 2 quaterdecies del D.lgs 196/2003 novellato dal D.lgs 101/2018 e considerando che tra i propri compiti rientra quello di autorizzare eventuali altri soggetti preposti al trattamento dei dati, con la presente

AUTORIZZA.....

AL TRATTAMENTO DEI DATI

Prescrizioni generali

Cosa sono i dati personali

''Il nuovo regolamento intende come dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile, si considera identificabile la persona 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".

Le persone fisiche possono essere associate ad **identificativi on line** prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli **indirizzi IP**, marcatori temporanei (**cookies**), o identificativi di altro tipo, come i **tag di identificazione a radiofrequenza**. Tali identificativi possono lasciare tracce che, in particolare, se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone e identificarle.

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, 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. In particolare:

- **dati genetici** 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;
- **dati biometrici** 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;
- **dati relativi alla salute** 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;

I dati giudiziari

I dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, *ad es.*, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione).

Cosa è il trattamento dei dati personali

Il GDPR definisce trattamento dei dati personali "qualunque operazione o complesso di operazioni, effettuati anche

senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati".

E' quindi indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati al regolamento.

Mansionario relativo al trattamento dei dati

a) Istruzioni operative generali

L'incaricato deve effettuare le operazioni di trattamento, che gli vengono affidate, nel rispetto delle disposizioni di legge, verificando in particolare che ai soggetti interessati sia stata data l'informativa pertinente allo specifico trattamento effettuato, che la stessa sia completa in tutte le sue parti e redatta ai sensi dell'art.13 del GDPR.

Nell'ambito della prescrizione generale, l'incaricato, coerentemente con quanto previsto dall'art. 5 del GDPR, deve trattare i dati secondo **liceità, correttezza e trasparenza**, accedendo esclusivamente alle banche dati e ai dati personali **necessari e pertinenti** allo svolgimento dei compiti che gli sono stati affidati e solo per scopi determinati e legittimi non eccedenti le sue mansioni (cosiddetto principio della minimizzazione dei dati).

L'incaricato è tenuto inoltre a partecipare a tutte le iniziative formative in materia di trattamento dei dati proposte dal Titolare del trattamento.

L'incaricato, inoltre, nell'eseguire le operazioni di trattamento deve rispettare le istruzioni di seguito specificate.

Rapporti di front-office.

Nel caso di rapporti di front – office deve:

- rispettare la **distanza di sicurezza:** per quanto riguarda gli operatori di sportello (cd. Front office) deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso invitare gli utenti a sostare dietro la linea tracciata sul pavimento, dietro le barriere delimitanti lo spazio di riservatezza o in caso di assenza di indicazioni diverse invitare gli utenti a mantenere una distanza adeguata;

- **identificazione dell'interessato**: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere (si pensi a soggetti stranieri ovvero a dati identificativi che possono generare dubbi sulla correttezza della registrazione) ovvero con riferimento alla personalità della prestazione richiesta: può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento, ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;

- **controllo dell'esattezza del dato:** fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbe creare problemi nella gestione dell'anagrafica e nel proseguo del processo;

- **obbligo di riservatezza e segretezza:** l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal Regolamento;

Cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:

- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazione di dati (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti; in altri casi, può essere utile comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);

- **verifica dell'esattezza dei dati comunicati:** nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione all'esattezza del dato che viene comunicato, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor.

Istruzioni per l'uso degli strumenti del trattamento

Telefono.

Non fornire dati e informazioni per telefono qualora non si abbia la certezza assoluta sull'identità del destinatario e che tale destinatario sia autorizzato. Qualora sia necessario, **accertarsi dell'identità** del diretto interessato prima di fornire informazioni circa i dati personali o il trattamento effettuato.

Nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:

- chiedere l'identità del chiamante e la motivazione della richiesta;
- richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
- verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante (ad esempio caserma dei carabinieri, servizi pubblici e di PS, …);
- procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza.

Fax.

Nell'utilizzare questo strumento occorre prestare attenzione a:

- digitare correttamente il numero di telefono, cui inviare la comunicazione;
- controllare l'esattezza del numero digitato prima di inviare il documento;
- verificare che non vi siano inceppamenti della carta ovvero che non vengano presi più fogli contemporaneamente;
- attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
- qualora vengano trasmessi dati idonei a rivelare lo stato di salute, può essere opportuno anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
- in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax.

Scanner.

I soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;

Distruzione delle copie cartacee.

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche), ovvero alla sostituzione della documentazione cartacea con registrazione ottica devono procedere alla distruzione controllata dei supporti cartacei non più occorrenti ovvero che presentino una forma non corretta. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto: si potranno utilizzare apparati distruggi documenti o altri sistemi atti a ciò;

b) Ambito del trattamento consentito

L'incaricato deve gestire i seguenti archivi e trattamenti:

Trattamenti	Natura dei dati	Archivi

I dati trattati, necessari per lo svolgimento delle mansioni lavorative, sono custoditi negli archivi, posti negli armadi degli uffici preposti. Tali archivi sono ad accesso selezionato, per cui potrà accedervi nei limiti in cui ciò sia strettamente necessario per prelevare e riporre i documenti necessari per lo svolgimento delle mansioni lavorative.

c) Trattamento con strumenti elettronici

Nello svolgimento dei suoi compiti, l'incaricato è autorizzato ad accedere all'elaboratore preposto al trattamento dei dati, previa verifica della sua identità. A tale fine:

1. Dovrà utilizzare un codice di identificazione (*username)*
2. Dovrà utilizzare una parola chiave (*password*), composta di otto caratteri alfanumerici che dovrà essere modificata almeno ogni sei mesi, nel caso in cui con l'elaboratore tratti solo dati di natura comune, o almeno ogni tre mesi, nel caso in cui con l'elaboratore tratti anche dati di natura particolare o giudiziaria.

La parola chiave:

a) deve essere mantenuta segreta, adottando gli opportuni accorgimenti per la sua custodia;
b) non deve contenere riferimenti agevolmente riconducibile alla sua persona e dovrebbe essere generata preferibilmente senza un significato compiuto;
c) deve essere composta da caratteri speciali e lettere maiuscole e minuscole;
d) non deve essere rivelata al telefono, né inviata via fax o e –mail o tramite cellulare, nessuno è autorizzato a richiederla

In particolare l'incaricato dovrà:

- utilizzare la credenziale di autenticazione, composta da Username e Password, provvedere a custodirla con la massima attenzione e segretezza, non divulgarla o comunicarla a terzi nel rispetto di quanto previsto dal GDPR;

- modificare la credenziale di autenticazione ogni volta che dovessero sorgere dei dubbi sulla sua segretezza;

- informare tempestivamente il Titolare/Responsabile del trattamento in caso di situazioni critiche dalle quali potrebbero verificarsi perdite o danneggiamenti dei dati trattati;

- impedire l'accesso non autorizzato ai dati provvedendo, nel caso di assenza anche momentanea dalla postazione di lavoro a chiudere preventivamente tutte le applicazioni in uso sul proprio elaboratore, oppure a porre la macchina in posizione di *stand-by,* adottando un sistema di oscuramento (cd. ***screen-saver***) dotato di password, o ancora a spegnere l'elaboratore che si sta utilizzando;

- per l'accesso a software e portali potrebbero essere previste ulteriori password, che devono seguire, in mancanza di ulteriori indicazioni o vincoli, le indicazioni sopra riportate;

- utilizzare i mezzi informatici, inclusa la posta elettronica (fornita dall'Azienda) e Internet, esclusivamente per scopi aziendali;

- non utilizzare a fini aziendali, a meno che ciò non sia permesso dal Titolare del trattamento o in caso di emergenza, la casella di posta elettronica personale a fini aziendali questo vale sia per web-mail che per caselle POP configurate su Outlook;

- non effettuare download di file o software, senza previa autorizzazione;

- non accedere a dati il cui contenuto sia dubbio o illecito né trasferirli nella rete del Titolare;

- impiegare sui PC solo software provvisti di licenza, acquistati dal Titolare;

- salvare i dati ed i file allegati ai messaggi di posta elettronica, negli archivi aziendali, secondo i criteri di archiviazione definiti;

- non salvare localmente (su disco "C") dati personali su PC collegati in rete, ma salvarli regolarmente su disco di rete con accesso vincolato;

- non accedere a servizi non consentiti; nel caso in cui fosse necessario per la propria attività di usufruire di tali servizi confrontarsi con l'Amministratore di Sistema;

- non caricare ed eseguire software di rete o di comunicazione, senza previa verifica dello stesso da parte dell'Amministratore di sistema;

- non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete del Titolare;

- custodire in luogo sicuro i dispositivi rimovibili (es. chiavette usb) contenenti dati personali. Prima di rottamare un qualsiasi dispositivo informatico (compresi i supporti rimovibili) l'incaricato deve cancellare eventuali dati personali contenuti nel dispositivo;

- procedere alla cancellazione dei supporti magnetici od ottici contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;

- la cancellazione dei dati contenuti nelle banche darti elettroniche deve avvenire previa autorizzazione del Titolare del trattamento o secondo le procedure definite. Potrà essere richiesta la verbalizzazione di tale atto. Nel caso di difficoltà nel compiere tali azioni dovrà essere richiesta la collaborazione dell'Amministratore di sistema o di altro soggetto autorizzato;

- nel caso in cui utilizzi dispositivi propri dovrà attenersi ad ulteriori misure di sicurezza, indicate dal Titolare del trattamento o da un suo delegato;

- in caso di furto, danneggiamento o perdita, anche accidentale dei dati o l'accesso abusivo agli strumenti a disposizione (anche personali) contenti dati aziendali dovrà comunicarlo immediatamente al Titolare in modo che possa attivare le procedure di **Data Breach**.

CRM e Banche dati

La visione dei dati, contenuti nelle banche dati, **esclude** comunque qualsiasi forma di comunicazione, diffusione e trattamento degli stessi che non sia strettamente funzionale all'espletamento dei compiti e che non si svolga nei limiti stabiliti da leggi e regolamenti

L'utilizzo della posta elettronica e internet

Per lo svolgimento delle sue mansioni lavorative, l'incaricato può utilizzare la casella di posta elettronica come strumento aziendali messo a disposizione ma, come tutti gli strumenti di lavoro, essi rimangono a completa e totale disponibilità dell'azienda.

Il Titolare del trattamento o, su suo mandato, l'Amministratore di sistema, può effettuare controlli sull'utilizzo dei sistemi di navigazione, per questioni di sicurezza con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi (nell'atto della navigazione l'incaricato/autorizzato al trattamento potrebbe involontariamente scaricare virus che potrebbero danneggiare l'utilizzo della rete aziendale o compromettere la sicurezza delle informazioni memorizzate con sistemi informatici).

Le caselle di posta aziendali nominative servono esclusivamente per l'uso e la trasmissione di dati aziendali, rimanendo comunque di proprietà della società, per questo si informa l'incaricato al trattamento che la trasmissione è controllata dal Titolare dei dati e che i messaggi inviati e ricevuti vengono automaticamente salvati sul server aziendale e in quello cloud di posta elettronica utilizzato per un periodo di dieci anni per poi essere distrutte, per ottemperare alle attività contrattuali anche prospect di modo da consentire al titolare di poter far fronte ad eventuali azioni giudiziarie reclami o lamentate inadempienze mosse da clienti.

Per quanto riguarda il flusso di dati, veicolati ad ogni livello, tramite posta elettronica è cura degli incaricati procedere alla loro archiviazione o distruzione proprio in virtù della natura personale del documento contenuto.

Si raccomanda di procedere al trasferimento dei dati importanti, sui supporti indicati dal Titolare, per quanto riguarda:

- mail di valore legale e contenenti informazioni che possono tornare utili nel tempo
- mail riguardanti ricevute di ritorno di avvenuta ricezione documenti e dati spediti
- altre mail che l'incaricato ritiene di dovere conservare

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile ribadire che:

- non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate,
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione, ecc.
- la posta elettronica può essere intercettata da estranei, e dunque non deve essere usata per inviare documenti di lavoro strettamente riservati. Ogni comunicazione (interna ed esterna), inviata o ricevuta,

che abbia contenuti rilevanti o contenga dati particolarmente sensibili o coperti dal segreto, deve essere autorizzata dal Responsabile o dal Titolare.

- In caso di assenza improvvisa e prolungata dell'incaricato e qualora vi sia la necessità per improrogabili necessità lavorative di accedere ai messaggi contenuti nella casella di posta elettronica assegnata all'incaricato, questo potrà delegare un altro lavoratore (fiduciario) per verificare il contenuto dei messaggi ed inoltrarli al responsabile. Della seguente attività si redigerà un apposito verbale ed di informerà l'incaricato alla prima occasione utile (rif linee guida del Garante per posta elettronica e internet G.U. n.58 del 10 marzo 2007) .

Alla conclusione del rapporto di lavoro la casella elettronica dell'incaricato al trattamento verrà bloccata in entrata ed in uscita e l'eventuale posta in arrivo verrà eliminata e inviato al mittente il riferimento di un nuovo indirizzo a cui mandare le comunicazioni.

Il contenuto della posta elettronica in ottemperanza alla politica sulla privacy aziendale verrà conservato per dieci anni per poi essere distrutto, per ottemperare alle attività contrattuali anche prospect di modo da consentire al titolare di poter far fronte ad eventuali azioni giudiziarie reclami o lamentate inadempienze mosse da clienti.

Nel caso in cui la posta elettronica usata sia di funzione e in condivisione con altri incaricati, alla conclusione del rapporto di lavoro la casella elettronica di funzione, a cui accedeva l'incaricato al trattamento, verrà resa accessibile al nuovo incaricato che verrà designato alla mansione. Si invita pertanto l'incaricato autorizzato di procedere alla cancellazione di eventuali informazioni e dati non connessi alla attività lavorativa.

Inoltre, specificatamente riguardo la *navigazione internet* è vietato:

- navigare su pagine internet che non riguardano l'ambito di lavoro e lasciano intendere le opinioni politiche, religiose o sindacali del collaboratore;
- effettuare operazioni finanziarie (Remote banking, acquisto on-line ecc.) se non hanno attinenza con l'ambito lavorativo e senza autorizzazione esplicita;
- il download di Freeware o Shareware senza autorizzazione esplicita del Titolare;
- la registrazione sulle pagine internet non concernente la sfera di competenza;
- la partecipazione a forum, chat, concorsi elettronici non concernenti l'ambito di lavoro e le iscrizioni nei Guest books (anche con pseudonimo).

d) Uso dei telefoni cellulari e dei personal computer portatili se forniti

Ogni incaricato al trattamento che riceve tali strumenti si impegna, dietro di firma di apposito modulo e oltre a quanto sopra indicato, a:

- utilizzare i mezzi esclusivamente per scopi aziendali;
- proteggere il contenuto tramite l'utilizzo rispettivamente del codice PIN (cellulari) e della Password (computer portatili) e a modificarle regolarmente secondo quanto indicato dal Titolare;
- proteggere da furto, perdita, danneggiamento e, in ogni caso segnalare al Titolare del trattamento il furto, la perdita o il danneggiamento dei mezzi resi disponibili dall'azienda. È vietato lasciare gli strumenti in luoghi incustoditi (es. bagagliaio auto in caso di sosta).

L'azienda si riserva la facoltà di disabilitarne l'utilizzo dei mezzi resi disponibili. Tali mezzi, infatti, sono strumenti aziendali messi a disposizione dell'incaricato al fine di consentirgli lo svolgimento della propria mansione ma, come tutti gli strumenti di lavoro, essi rimangono nella completa e totale disponibilità dell'azienda.

Alla cessazione del rapporto di lavoro gli strumenti vanno riconsegnati al Titolare del trattamento. Gli eventuali dati personali dell'incaricato al trattamento non connessi alla attività lavorativa vanno cancellati.

E' facoltà della società effettuare controlli che siano conformi ai principi di necessità, pertinenza e non eccedenza del trattamento, sui dispositivi dati in dotazione nel pieno rispetto della normativa privacy vigente.

e) Uso delle chiavi e dei badge se forniti

Ogni incaricato al trattamento che riceve tali strumenti si impegna, a proteggerli da furto, perdita, danneggiamento e,

in ogni caso segnalare al Titolare del trattamento il furto, la perdita o il danneggiamento. È vietato lasciarli in luoghi incustoditi.

L'azienda si riserva la facoltà di disabilitarne l'utilizzo e/o ritirare i mezzi resi disponibili. Tali mezzi, infatti, sono strumenti aziendali messi a disposizione dell'incaricato al fine di consentirgli lo svolgimento della propria mansione ma, come tutti gli strumenti di lavoro, essi rimangono nella completa e totale disponibilità dell'azienda.

Alla cessazione del rapporto di lavoro gli strumenti vanno riconsegnati al Titolare del trattamento responsabile badge,

f) Utilizzo dei byod (Bring your own device – porta il tuo dispositivo) se permessi

Qualora un incaricato sia stato espressamente autorizzato dalla società all'utilizzo di dispositivi elettronici personali durante le attività lavorative, premesso che la società è "Titolare del trattamento" relativamente ai dati che sono trattati per suo conto da parte dell'incaricato al trattamento, occorre che si uniformi alle sottostanti prescrizioni, pena l'applicazione di sanzioni.

a) i dati trattati devono risiedere solo sulle infrastrutture informatiche e quindi non è consentito scaricare i dati/file/archivi sui dispositivi personali

b) i dati personali degli interessati non devono essere trattati per scopi differenti da quelli per cui sono stati originariamente raccolti e devono essere utilizzati solo per il tempo necessario

c) deve essere assolutamente evitata la disseminazione indistinta (ad esempio su più dispositivi) dei dati personali oggetto di trattamento tramite BYOD

d) l'accesso ai dispositivi deve essere regolamentato da apposite credenziali (es: password o PIN)

e) qualora il dispositivo personale che contiene dati del Titolare del trattamento, fosse perso, smarrito, rubato, fosse oggetto di un accesso improprio o comunque ci sono elementi per immaginare/sospettare che i dati contenuti possano essere, sia pure temporaneamente, resi accessibili a terze parti, l'incaricato deve informare immediatamente il Titolare del trattamento affinché possa essere valutata la problematica e prese, se del caso le opportune misure. La comunicazione deve essere immediata e non possono esser accettati ritardi

f) nel caso in cui il dispositivo mobile del lavoratore sia venduto, ceduto, trasferito, il contenuto deve essere cancellato/anonimizzato in modo irreversibile.

g) Trattamenti senza strumenti elettronici

Per quanto riguarda la eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali, gli atti e i documenti contenenti i dati devono essere conservati, dalle persone autorizzare al trattamento dei dati personali, per la durata del trattamento e successivamente riposti in archivi ad accesso controllato, al fine di escludere l'accesso, agli stessi, da parte di persone non incaricate al trattamento o, in mancanza chiudere a chiave l'ufficio nel quale si effettua il trattamento se gli archivi sono in esso contenuti.

Nel caso di trattamento di dati sensibili, di dati di minori o di dati giudiziari, gli atti e i documenti, contenenti i dati affidati alle persone autorizzate al trattamento, devono essere conservati in contenitori muniti di serratura, al fine di escludere l'acquisizione, degli stessi, da parte di persone non autorizzate del trattamento.

La cancellazione dei dati contenuti negli archivi cartacei deve avvenire secondo i tempi/criteri contenuti nel "Registro dei Trattamenti" e previa autorizzazione del Titolare del trattamento. Potranno essere richieste la verbalizzazione di tale atto. Quando è necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili;

Le persone autorizzate al trattamento sono tenute a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto

L'incaricato si impegna a:

- verificare che i documenti utilizzati siano sempre sotto il suo controllo e la sua custodia per l'intero ciclo necessario allo svolgimento delle operazioni relative al trattamento dei dati, al fine di garantire che i documenti non siano visti o trattati da persone non autorizzate;
- conservare i documenti, in caso di trasferimento degli stessi, in contenitori chiusi ed anonimi;

- effettuare le copie dei dati documenti cartacei solo se strettamente necessario ed in ogni caso trattarle con la stessa cura dei documenti originali, al termine del trattamento distruggere eventuali copie non utilizzate o comunque alterarle per impedirne la consultazione;
- controllare che i documenti, composti da numerose pagine o più raccoglitori, siano sempre completi, verificando che sia il numero dei fogli sia l'integrità del contenuto è conforme a quanto era presente all'atto del prelievo dal luogo sicuro;
- identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati. Ove si utilizzi un contenitore, un armadio o un raccoglitore chiuso a chiave, l'incaricato deve custodire le chiavi, ed accertarsi che non esistano duplicati abusivi delle stesse;
- utilizzare buste di sicurezza con chiusura auto sigillante, per la consegna di copie di documenti, se possibile eseguire la consegna personalmente al fine di ridurre al minimo la possibilità che, soggetti terzi non autorizzati, possano prendere visione del contenuto a addirittura fotocopiarlo all'insaputa del mittente e destinatario,
- non discutere, comunicare o trattare dati personali per telefono se non si è certi che il corrispondente sia un Incaricato, il cui profilo di autorizzazione sia tale da consentire l'acquisizione e il trattamento dei dati in oggetto. Questa precauzione diventa indispensabile se l'apparecchio è utilizzato in luogo pubblico o aperto al pubblico.
- non parlare mai ad alta voce, trattando dati personali, in presenza di terzi non autorizzati che potrebbero venire a conoscenza di dati personali in modo fortuito e accidentale.
- custodire le chiavi, se si utilizza un armadio e/o un contenitore con serratura, ed accertarsi che non esistano duplicati abusivi delle stesse.

L'incaricato dichiara:

- di essere a conoscenza degli obblighi derivanti da quanto di seguito riportato e da qualsiasi altro obbligo riportato nel suo mansionario;
- di essere a conoscenza che in caso venissero riscontrate azioni illecite o il mancato rispetto delle istruzioni contenute nel presente documento, il Titolare del trattamento si riserba di provvedere ad azioni disciplinari nei suoi confronti nel caso in cui gli possono essere imputate (in maniera lampante) le predette azioni illecite, sempre e comunque secondo le regole previste dal C.C.N.L. e dallo statuto dei lavoratori.

In ordine alla durata della nomina, si fa presente che la revoca della stessa avverrà con la risoluzione del contratto di lavoro posto in essere tra il Titolare del trattamento e l'Incaricato. Tuttavia, il Titolare si riserva di verificare un eventuale cambio di ruolo, mansione o ufficio che determini una modifica della tipologia di dati trattati dall'incaricato. In tal caso si procederà con la stipula di una lettera di revisione che definisca il nuovo ambito di trattamento.

L'incaricato con la firma della presente lettera accetta la nomina e conferma di aver preso conoscenza del presente accordo come parte integrante del contratto di lavoro e di osservarne le disposizioni nello svolgimento del proprio lavoro.

Titolare del trattamento

_____

9. ALLEGATO N. 2 - FAC – SIMILE CONTRATTO RESPONSABILE ESTERNO

ATTO DI NOMINA E

ACCORDO PER IL TRATTAMENTO DATI

IL PRESENTE ACCORDO È CONCLUSO TRA:

…….

E

…….

di seguito, individualmente la **"Parte"** e congiuntamente le **"Parti"**.

PREMESSO CHE:

- Le Parti riconoscono ed accettano, che per il Responsabile potrebbe rendersi necessario trattare alcuni Dati Personali per conto del Titolare;
- In virtù di tale trattamento, e al fine di consentire al Titolare di rispettare gli obblighi normativi allo stesso imposti dal Regolamento 2016/679 (di seguito, anche "GDPR") e da ogni altra Legge Applicabile, le Parti hanno convenuto di stipulare il presente Accordo;
- **…….** è incaricato dalla **…….** a Trattare Dati Personali per conto della stessa in qualità di Responsabile del trattamento dei dati personali e a fornire i Servizi conformemente a quanto previsto dal presente Accordo; tale nomina viene effettuata dalla **…….** ai sensi dell'art. 28 del GDPR.

Le Parti convengono quanto segue:

1. DEFINIZIONI

Nel presente Accordo:

"Contratto"	si intende il Contratto sottoscritto con il quale il responsabile assume l'incarico assegnato dal titolare del trattamento
"Autorità Privacy"	si intende l'autorità di controllo responsabile per la protezione dei dati personali nell'ambito della giurisdizione a cui il Titolare è soggetto
"Dati Personali"	si intendono tutte le informazioni relative ad una persona fisica identificata o identificabile secondo quanto definito dalla Legge Applicabile
"GDPR" o "Regolamento"	si intende il Regolamento UE 2016/679 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e della loro libera circolazione (General Data Protection Regulation) che sarà direttamente applicabile dal 25 maggio 2018
"Misure di Sicurezza Minime"	si intendono le prescrizioni minime di sicurezza del Titolare, e che possono essere aggiornate ed implementate di volta in volta, in conformità alle previsioni del presente Accordo
"Legge Applicabile"	si intende l'insieme delle norme rilevanti in materia protezione dei dati personali, incluso il Regolamento Privacy UE 2016/679 (GDPR), alle quali Titolare è soggetto, ed ogni linea guida, codice o provvedimento rilasciato o emesso dalla/e Autorità Privacy
"Titolare del Trattamento"	si intende la società che determina le finalità e le modalità di Trattamento dei Dati Personali
"Trattamento"	si intende qualunque operazione o complesso di operazioni effettuata su Dati Personali attraverso, o meno, l'utilizzo di strumenti automatizzati, comprese le operazioni di raccolta, registrazione, organizzazione, memorizzazione, adattamento, alterazione, recupero, consultazione, utilizzo, divulgazione, messa a disposizione, aggiornamento, associazione, blocco, cancellazione e distruzione dei Dati Personali ai

	sensi della Legge Applicabile

2. TRATTAMENTO DEI DATI NEL RISPETTO DELLE ISTRUZIONI DEL TITOLARE DEL TRATTAMENTO

Il responsabile, relativamente a tutti i Dati Personali che tratta per conto del Titolare, garantisce che:

- tratterà tali Dati Personali solo ai fini dell'esecuzione del presente Contratto e solo nel rispetto di quanto eventualmente concordato dalle Parti, agendo pertanto, esclusivamente sulla base delle istruzioni documentate e fornite dal Titolare. In particolare, Il responsabile non eserciterà alcun controllo sui Dati Personali, e pertanto, non potrà trasferire gli stessi a terzi soggetti, ad eccezione del caso in cui tale possibilità sia specificatamente autorizzata dal Titolare per iscritto;
- non tratterrà Dati Personali per proprie finalità;
- prima di iniziare ogni trattamento e, ove occorra, in qualsiasi altro momento, informerà il Titolare se, a suo parere una qualsiasi istruzione fornita dal Titolare si pone in violazione di legge.
- Il responsabile è soggetto al rispetto di previsioni di legge, che potrebbero rendere per lo stesso, in tutto o in parte, impossibile o illegale agire conformemente alle istruzioni impartite dal Titolare o nel rispetto di quanto previsto dalla Legge Applicabile.

Al fine di garantire il rispetto delle istruzioni impartite dal Titolare, secondo quanto previsto dal presente articolo, il responsabile si avvarrà di adeguati processi e di ogni altra misura tecnica idonea ad attuare le istruzioni fornite dal Titolare, incluse:

- le procedure idonee a garantire il rispetto dei diritti e delle richieste formulate al Titolare dagli interessati relativamente ai loro Dati personali;
- l'adozione di adeguate interfacce o sistemi di supporto che consentano di garantire e fornire informazioni agli interessati così come previsto dalla Legge Applicabile;
- procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta del Titolare, dei Dati Personali di ogni interessato;
- procedure atte a garantire la cancellazione o il blocco dell'accesso ai Dati Personali a richiesta del Titolare;
- procedure atte a garantire il diritto degli Interessati alla limitazione di trattamento, su richiesta del Titolare.

Il responsabile deve rispettare la Legge Applicabile e deve adempiere agli obblighi previsti dal presente Accordo in modo da evitare che il Titolare incorra nella violazione di un qualunque obbligo previsto dalla Legge Applicabile.

Il responsabile deve garantire e fornire al Titolare cooperazione, assistenza e le informazioni che potrebbero essere ragionevolmente richiesti dallo stesso, per consentirgli di adempiere ai propri obblighi ai sensi della Legge Applicabile.

Il responsabile si impegna inoltre a rispettare le indicazioni o le decisioni provenienti da un'Autorità Privacy entro un tempo utile che consenta al Titolare di rispettare il termine imposto dalla stessa Autorità Privacy.

Le Parti riconoscono e convengono che Il responsabile non avrà diritto di rimborso delle eventuali spese, che lo stesso potrebbe dover sostenere per essersi attenuto alle istruzioni impartite dal Titolare, per l'esecuzione del Contratto, e/o di un qualsiasi altro suo obbligo previsto dall'Accordo o da qualsiasi altra Legge Applicabile.

Il responsabile, anche nel rispetto di quanto previsto all'art. 30 del Regolamento, deve mantenere e compilare, in proprio e/o in base alle indicazioni che verranno fornite dal Titolare, e rendere disponibile a richiesta dello stesso, un registro dei trattamenti dati personali, effettuati dallo stesso, laddove tali trattamenti non siano altrimenti documentati.

Tale registro deve includere:

- il nome e i dati di contatto del responsabile; di ogni Titolare del trattamento per conto del quale opera il responsabile e del Responsabile della protezione dei dati ove presente;
- le categorie di trattamento effettuate per conto di ciascun titolare del trattamento;
- se del caso, i trasferimenti dei Dati Personali verso un paese terzo o ad un'organizzazione internazionale, compresa l'individuazione e l'indicazione di questi ultimi.

Il responsabile, al fine di consentire al Titolare di effettuare una valutazione di impatto sulla protezione dei dati personali, che si rende necessaria ogni qual volta un determinato trattamento potrebbe rivelare un rischio elevato per i diritti e le libertà delle persone fisiche, nonché di rispettare quanto previsto all'art. 35 del Regolamento, si impegna a supportare e a mostrare la massima collaborazione a richiesta del Titolare, al fine di esperire tale tipo di attività.

3. PROTEZIONE DEI DATI PERSONALI

Il responsabile deve conservare i Dati Personali garantendo la separazione di tipo logico dai dati Personali trattati per

conto di terze parti o per proprio conto.

Il responsabile deve adottare e mantenere appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i Dati Personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati, ed in particolare, laddove il trattamento comporta trasmissioni di dati su una rete, da qualsiasi altra forma illecita di trattamento.

A tal fine il Responsabile si impegna a rispettare i Requisiti Minimi di Sicurezza previsti dal Titolare in materia di protezione dei dati personali e i provvedimenti in materia del Garante per la protezione dei dati personali, ivi incluso il provvedimento del 27 novembre 2008 in materia di amministratori di sistema, fatti salvi gli adeguamenti che potranno essere necessari a seguito dell'applicazione del Regolamento e di suoi eventuali provvedimenti attuativi.

4. SICUREZZA DELLE COMUNICAZIONI

Il responsabile deve adottare misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti al Titolare o utilizzati per trasferire o trasmettere i Dati Personali (incluse, ad esempio, le misure intese a garantire la segretezza delle comunicazioni così da prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema), garantendo, in tal modo, la sicurezza delle comunicazioni.

5. INCARICATI DEL TRATTAMENTO - RISERVATEZZA

Il responsabile garantisce l'affidabilità di qualsiasi dipendente e Sub-Responsabile o Sub-Fornitore che accede ai Dati Personali del Titolare ed assicura, inoltre, che gli stessi abbiano ricevuto adeguata formazione con riferimento alla protezione e gestione dei Dati Personali, e che siano vincolati al rispetto di obblighi di riservatezza non meno onerosi di quelli previsti nel presente Accordo relativamente al Trattamento dei Dati Personali.

In ogni caso il responsabile sarà direttamente ritenuto responsabile per qualsiasi divulgazione dei Dati Personali dovesse realizzarsi ad opera di tali soggetti.

6. TRATTAMENTO DEI DATI PERSONALI FUORI DALL'AREA ECONOMICA EUROPEA –

Laddove i Dati Personali originari dell'Area Economica Europea vengano trattati dal responsabile o da altri Sub-Responsabili o Sub-Fornitori, al di fuori dello spazio economico europeo, o in un territorio che non garantisce un adeguato livello di protezione dei dati riconosciuto dalla Commissione europea, questo dovrà essere preventivamente notificato al Titolare.

7. SUB-RESPONSABILI DEL TRATTAMENTO DI DATI PERSONALI

Il responsabile non può, ai sensi del presente Accordo, sub-appaltare o esternalizzare un qualsiasi Trattamento dei Dati Personali a qualsiasi altro soggetto a condizione che:

- Il responsabile abbia notificato per iscritto al Titolare il nome completo, la sede legale o la sede principale degli affari del Sub-Fornitore e/o Sub-Responsabile mediante la compilazione dell'Allegato 1;
- Il responsabile abbia fornito al Titolare ogni altra informazione che potrebbe rendersi necessaria per consentire alla stessa di conformarsi alla Legge Applicabile, permettendogli, ad esempio, di inviare la notificazione all'Autorità Privacy competente, laddove necessaria;
- Il responsabile abbia imposto al Sub-Fornitore e/o al Sub-Responsabile condizioni vincolanti in materia di trattamento dei Dati Personali non meno onerose di quelle contenute nel presente Accordo;
- Il Titolare non si sia opposto all'esternalizzazione, entro i successivi 7 sette giorni lavorativi dalla ricezione della notifica scritta del Responsabile già indicata;

Qualora richiesto dal Titolare, il responsabile dovrà provvedere a che ogni Sub-Fornitore e/o Sub- responsabile, incaricato dal responsabile stesso ai sensi del presente articolo, sottoscriva un accordo di trattamento dei dati con Titolare, che preveda sostanzialmente gli stessi termini del presente Accordo.

Il responsabile concorda che tutte le modifiche alle informazioni presenti nell'Allegato 1 dovranno essere notificate a Titolare in conformità a quanto previsto nel presente articolo.

In tutti i casi, il "responsabile del trattamento" resta responsabile nei confronti del Titolare per qualsiasi atto od omissione realizzati da un Sub-fornitore, da un Sub-Responsabile o da altri terzi soggetti incaricati dallo stesso, indipendentemente dal fatto che il responsabile abbia o meno rispettato i propri obblighi.

In caso di violazione del presente Accordo causata dalla condotta o da azioni di un Sub- fornitore e/o di un Sub-Responsabile, il responsabile se richiesto dal Titolare, riconosce e attribuisce al Titolare il diritto di agire sostituendosi allo stesso nel contratto con il Sub-Fornitore e/o con il Sub-Responsabile, così da poter esercitare tutte le azioni che

riterrà necessarie al fine di salvaguardare i Dati Personali.

8. VIOLAZIONE DEI DATI PERSONALI E OBBLIGHI DI NOTIFICA

Il responsabile, in virtù di quanto previsto dall'art. 33 del Regolamento, nonché nel rispetto del provvedimento dell'Autorità Privacy italiana n. 97 del 4 aprile 2013, dovrà notificare al Titolare nel minor tempo possibile, e comunque non oltre 72 ore da quando ne abbia avuto conoscenza, qualsiasi distruzione, perdita, alterazione, divulgazione o accesso non autorizzato ai Dati personali ("Violazione della sicurezza") ivi incluse quelle che abbiano riguardato i propri sub-Fornitori e/o sub-Responsabili.

Tale notifica deve contenere:

- ✓ una descrizione dettagliata della Violazione della sicurezza,
- ✓ il tipo di dati che è stato oggetto di Violazione della sicurezza
- ✓ l'identità di ogni interessato (o se non è possibile, il numero approssimativo delle persone interessate e i dati personali coinvolti.).

Il responsabile deve poi comunicare al Titolare:

- il nome e i contatti del proprio Responsabile della protezione dei dati, o i recapiti di un altro punto di contatto attraverso cui è possibile ottenere ulteriori informazioni;
- una descrizione delle probabili conseguenze della Violazione della sicurezza;
- una descrizione delle misure adottate o che si intende adottare per affrontare la Violazione della sicurezza, compreso, ove opportuno, misure per mitigare i suoi possibili effetti negativi;
- non appena possibile, ogni altra informazione raccolta o resa disponibile, nonché ogni altra informazione che possa essere ragionevolmente richiesta da Titolare relativamente alla Violazione della sicurezza.

Qualora Il responsabile non possa fornire con la notifica le informazioni di cui sopra, per ragioni che sfuggono alla sua sfera di controllo, le informazioni devono essere trasmesse non appena possibile.

Il responsabile deve attivarsi immediatamente per indagare sulla Violazione della sicurezza e per individuare, prevenire e limitare gli effetti negativi di tale violazione, conformemente ai suoi obblighi ai sensi del presente articolo e, previo accordo del Titolare, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa.

Nel caso in cui la Violazione della Sicurezza avesse un impatto maggiore sui dati del responsabile, quest'ultimo dovrà comunque dare priorità al Titolare nel fornire il proprio supporto ed attuare i rimedi e le azioni che si riterranno necessarie.

9. ANALISI DEI RISCHI, PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Qualora sia richiesto dal Titolare, il responsabile deve rendere disponibili tutte le informazioni necessarie per dimostrare la conformità del Titolare alla Legge Applicabile e deve assisterlo nelle attività di valutazione di impatto e dei connessi trattamenti di dati, nonché collaborare al fine di dare effettività alle azioni di mitigazione previste e concordate per affrontare eventuali rischi identificati.

Il responsabile dovrà fare tutto il possibile per consentire al Titolare di rispettare le previsioni di cui all'art. 25 del Regolamento relativamente alla protezione dei dati fin dalla progettazione (c.d. privacy by design) nonché alla protezione per impostazione predefinita (c.d. privacy by default).

In particolare, in linea con i principi di privacy by design, ogni nuovo trattamento dovrà essere progettato in modo da garantire una sicurezza adeguata alla luce dei rischi relativi allo specifico trattamento. Inoltre, Il responsabile dovrà consentire al Titolare, tenuto conto dello stato della tecnica, dei costi, della natura, dell'ambito e della finalità del relativo trattamento, di adottare, sia nella fase iniziale di determinazione dei mezzi di trattamento, che durante il trattamento stesso, ogni misura tecnica ed organizzativa che si riterrà opportuna per garantire ed attuare i principi previsti in materia di protezione dati e a tutelare i diritti degli interessati.

In linea con i principi di privacy by default, dovranno essere trattati, per impostazione predefinita, esclusivamente quei dati personali necessari per ogni specifica finalità del trattamento.

10. CANCELLAZIONE DEI DATI PERSONALI

Il responsabile provvede alla cancellazione dei Dati Personali trattati al termine del periodo di conservazione stabilito e in qualsiasi circostanza in cui sia richiesto dal Titolare, compresa l'ipotesi in cui la stessa debba avvenire su esercizio del relativo diritto dell'Interessato.

Alla cessazione del presente Accordo, per qualsiasi causa essa avvenga, i Dati Personali dovranno, a discrezione del

Titolare, essere distrutti o restituiti allo stesso, unitamente a qualsiasi supporto fisico o documento contenente dati personali di titolarità del Titolare.

11. RICHIESTE DI DIVULGAZIONE DEI DATI PERSONALI PER FINALITA D'INDAGINI E DIFENSIVE PROVENIENTI DA TERZE PARTI

Se non vietato dalla Legge Applicabile, il Responsabile o qualsiasi Sub-fornitore e/o Sub-Responsabile informa tempestivamente il Titolare, e in ogni caso entro due giorni lavorativi, di qualsiasi richiesta, comunicazione, o reclamo ricevuto da qualsiasi autorità di regolamentazione o di vigilanza o da qualsiasi interessato, relativamente ad ogni Dato Personale o ad ogni obbligo ai sensi della Legge Applicabile, e fornisce gratuitamente tutta la dovuta assistenza al Titolare per garantire che la stessa possa rispondere a tali comunicazioni o reclami e rispettare i termini temporali, previsti dalla legge e dai regolamentari applicabili.

12. RESPONSABILITA' E MANLEVE

Il responsabile tiene indenne e manlevato il Titolare da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura (sia essa prevedibile, contingente o meno) derivante o in connessione con una qualsiasi violazione da parte del responsabile delle disposizioni contenute nel presente Accordo. In particolare, il responsabile tiene indenne il Titolare da qualsiasi perdita derivante da qualsiasi violazione dei termini del presente Accordo o della Legge Applicabile, anche da parte di ogni Sub-fornitore e/o Sub-Responsabile di cui si avvale.

Il Titolare dovrà indennizzare il responsabile per ogni Reclamo sollevato contro quest'ultimo, per qualsiasi violazione della Legge Applicabile, che derivi esclusivamente dall'aver eseguito le istruzioni fornite dal Titolare ai sensi delle disposizioni del presente Accordo, sempre a condizione tuttavia che il responsabile abbia notificato al Titolare, preventivamente ed in forma scritta, che le istruzioni del Titolare avrebbero potuto comportare la violazione della Legge Applicabile e che lo stesso, nonostante la notifica del responsabile, abbia comunque ratificato le sue istruzioni in forma scritta.

A fronte della ricezione di un Reclamo relativo alle attività oggetto del presente Accordo, Il responsabile, avverte prontamente ed in forma scritta, il Titolare del Reclamo una volta che venga a conoscenza di esso e fornisce al Titolare tutta l'assistenza che potrebbe ragionevolmente richiedere nella gestione del Reclamo.

13. DURATA

Il presente Accordo decorre dalla data della sua sottoscrizione e rimarrà in vigore ed effetto fino alla risoluzione o scadenza del Contratto.

14. APPLICAZIONE DELL'ACCORDO

In deroga a quanto previsto all'art. 14, qualora il presente Accordo sia sottoscritto prima del 25 maggio 2018, esso troverà applicazione solo a partire da tale data. In tal caso, fino al 25 maggio 2018, i trattamenti di dati personali posti in essere dal responsabile per conto del Titolare saranno disciplinati dall'Atto di nomina a Responsabile del trattamento già in vigore.

Luogo e data

Firma Titolare Firma Responsabile

ALLEGATO 1 – LISTA DI SUB-RESPONSABILI APPROVATI

NOME DEL SUB RESPONSABILE	SEDE LEGALE	LUOGO DEL TRATTAMENTO	TIPO DI TRATTAMENTO EFFETTUATO

ALLEGATO 2 APPENDICE sul TRATTAMENTO dei DATI PERSONALI

Questa Appendice descrive i tipi di dati personali e gli scopi per i quali gli stessi possono essere trattati dal Responsabile del Trattamento.

Categorie speciali di dati personali:

Nessuna tipologia di dati personali appartenenti alle categorie particolari di cui all'art. 9 del Regolamento (es. dati che rivelino l'origine razziale, le opinioni politiche, le convinzioni filosofiche o religiose, lo stato di salute, ecc.), saranno trattati per gli scopi di cui al presente Allegato:

Attività di trattamento dei dati personali

FINALITA' DEL TRATTAMENTO	NATURA DEI DATI	ARCHIVI	SUB - RESPONSABILI APPROVATI	PERIODO DI CONSERVAZIONE DEI DATI PERSONALI

10. ALLEGATO N.3 – PROCEDURA DATA BREACH

1. PREMESSA

L' Istituto, ai sensi del Regolamento Europeo 2016/679, è tenuta a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (incluse eventuali notifiche all'Autorità Garante competente ed eventuali comunicazioni agli interessati).

È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, ciò al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'Azienda/Ente e per poter riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e/o gli interessati.

Le sanzioni previste dal Regolamento per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 del Regolamento, può comportare l'applicazione in capo al Titolare del trattamento una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del "fatturato" annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.

2. SCOPO DELLA PRESENTE PROCEDURA

Lo scopo di questa procedura è definire un flusso per la gestione delle violazioni dei dati personali trattati dall'Azienda/Ente. Queste procedure sono ad integrazione delle procedure e regolamenti eventualmente adottati dal Titolare del trattamento in materia di protezione dei dati personali ai sensi della legislazione vigente.

3. COS'E' UNA VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali è ogni infrazione alla sicurezza degli stessi che comporti - 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 dal Titolare del trattamento, anche qualora rivesta il ruolo di Responsabile (§5).

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

4. GESTIONE DELLA VIOLAZIONE

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato, sotto la supervisione del RPD/DPO qualora nominato.
In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.
Di seguito si riportano gli steps da seguire per una corretta gestione delle violazioni:

STEP	ATTIVITA'	CHI	QUANDO	COME
1	Rilevazione e segnalazione di data breach	Tutti: il personale, collaboratori, fornitori, responsabili nominati	Appena se ne viene a conoscenza	Informare il Referente privacy/Titolare del trattamento/Direzione utilizzando le vie più brevi (telefono, di persona, e-mail)
2	Analisi tecnica dell'evento ed eventuale registrazione della violazione	Titolare, Referente Privacy, RPD/DPO (ove nominato)	Al momento della venuta a conoscenza della violazione	Verificare se l'evento segnalato si configuri effettivamente come una violazione/ "Data Breach" (analisi preliminare). Annotare sul registro (**REGISTRO DELLE VIOLAZIONI**) la violazione subita, anche nel caso in cui dall'analisi preliminare emerga che la segnalazione non ha i caratteri di un Data Breach. Copia del registro dovrà essere inviata dalla/alla PEC istituzionale per l'applicazione della **data certa,** alla rilevazione dell'evento.
3	Raccolta informazioni sulla violazione	Il Referente Privacy insieme ai soggetti coinvolti nella violazione (o delegando l'attività, dando istruzioni precise per iniziare subito la raccolta delle informazioni, indicando dove reperire il modello predisposto a tale scopo)	Appena ricevuta l'informazione	In caso di effettiva violazione raccogliere gli ulteriori elementi per una valutazione approfondita dell'evento, utilizzando il modello fornito e raccogliendo ogni informazione dai soggetti coinvolti nella segnalazione e nel trattamento dei dati violati **ALLEGATO – MODULO RACCOLTA INFORMAZIONI**
4	Valutazione d'impatto	Il Referente Privacy, RPD/DPO (ove nominato), Tecnico informatico, soggetti coinvolti	Appena ricevuta l'informazione	Utilizzando: - il modello fornito per la valutazione di impatto **ALLEGATO - MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH** - Le indicazioni riportate nel §6.2 del presente documento (esempi)
5	Individuazione delle azioni correttive	Il Referente Privacy, RPD/DPO (ove nominato), Tecnico informatico, Direzione	Appena terminata la valutazione d'impatto	Analizzando i risultati della valutazione d'impatto (**MODULO DI VALUTAZIONE DEL RISCHIO** compilato)
6	Comunicazione delle valutazioni effettuate e delle azioni da intraprendere	Il Referente Privacy, RPD/DPO (ove nominato) o delegato, Direzione		Informare la Direzione delle valutazioni effettuate e delle azioni individuate, tramite una breve relazione anche orale

STEP	ATTIVITA'	CHI	QUANDO	COME
7	Notifica della violazione (se necessaria)	Titolare del trattamento	**Entro 72 ore** dalla rilevazione, ove sia probabile che la violazione **presenti un rischio (anche semplice, non nullo)** per i diritti e le libertà delle persone fisiche	Invio della notifica della violazione **al Garante della protezione dei dati personali,** mediante la modulistica predisposta dal Garante e/o invio di notifica all'indirizzo protocollo@pec.gpdp.it **Per la compilazione si rimanda al § 7.1.** **Invio della notifica anche al DPO (se nominato)**
8	Comunicazione agli interessati coinvolti (se necessaria)	Titolare del trattamento	Nei termini indicati nella valutazione d'impatto e comunque quando la violazione presenta un **rischio ELEVATO** per i diritti e le libertà delle persone fisiche	Comunicazione alle persone fisiche i cui dati sono stati violati mediante comunicazione diretta alle singole persone oppure mediante pubblicazione in sito a loro accessibile, delle eventuali conseguenze della violazione e sulle categorie di dati interessati.
9	Disposizioni per l'attuazione delle misure correttive (se individuate)	Titolare, Direzione, Referente Privacy, RPD/DPO (ove nominato), Tecnico informatico, soggetti coinvolti	Nei tempi indicati nella valutazione di impatto	Ai soggetti incaricati di svolgere le attività individuate come misure correttive, devono essere indicate in dettaglio le operazioni da svolgere, chi è l'incaricato, i tempi di attuazione; prevedere eventuali operazioni di verifica dell'efficacia delle misure correttive
10	Registrazione della violazione/aggiornamenti	Titolare, Referente Privacy, RPD/DPO (ove nominato)	Appena ricevuta l'informazione	Compilando l'apposito registro (**REGISTRO DELLE VIOLAZIONI**) con la descrizione delle informazioni aggiuntive inerenti alla violazione subita, delle azioni intraprese e annotando i successivi aggiornamenti fino alla completa risoluzione. Copia del registro dovrà essere inviata dalla/alla PEC istituzionale per l'applicazione della **data certa** alla conclusione della gestione dell'evento.
11	Recepimento della risposta del Garante alla notifica (se effettuata)	Titolare, Direzione, Referente Privacy, RPD/DPO (ove nominato), Tecnico informatico, soggetti coinvolti		Disposizioni per l'attuazione delle eventuali misure correttive indicate dal Garante; effettuazione di ulteriori indagini per approfondire le informazioni raccolte
12	Registrazione della risposta del Garante	Titolare, Direzione, Referente Privacy, RPD/DPO (ove nominato)	Al momento della ricezione	Annotando sul registro (**REGISTRO DELLE VIOLAZIONI**) gli estremi della risposta del Garante e le eventuali prescrizioni in essa contenute

STEP	ATTIVITA'	CHI	QUANDO	COME
13	Archiviazione	Titolare, Direzione, o suo delegato, Referente Privacy, RPD/DPO (ove nominato)	A conclusione dell'evento	La documentazione generata per la gestione di ogni violazione dovrà essere archiviata nell'apposita cartella (elettronica -**ARCHIVIO DELLE VIOLAZIONI**) riportando il numero progressivo (indicato nel registro delle violazioni) e l'anno di riferimento
14	Attività di miglioramento	Titolare, Direzione, Referente Privacy, RPD/DPO (ove nominato)	A conclusione dell'evento	Verificare l'efficacia delle azioni correttive effettuate e verificare la necessità di eventuali azioni di miglioramento

5. GESTIONE DELLA VIOLAZIONE IN QUALITA' DI RESPONSABILE ESTERNO

Le operazioni, come riportate in tabella, sono da intendersi applicabili anche qualora si rivesta il ruolo di Responsabile esterno nominato dal Titolare del trattamento per lo svolgimento di determinate operazioni di trattamento.
Come precisato meglio nei documenti di nomina di volta in volta sottoscritti, **nel caso in cui si ravvisi una violazione dei dati gestiti in qualità di responsabile, è il Titolare a definire le procedure, le modalità, i tempi e referenti con le quali questa deve essere a Lui comunicata.**
Restano escluse, quindi, le attività di comunicazione all'Autorità e di comunicazione agli interessati coinvolti; l'adempimento di questi obblighi restano in capo al Titolare del trattamento.

6. VALUTAZIONE DI IMPATTO ED ESEMPI DI DATA BREACH

6.1 Valutazione di impatto di una violazione

Sebbene il Regolamento introduca l'obbligo di notificare una violazione, non è obbligatorio farlo in tutte le circostanze:

- la notifica all'autorità di controllo competente è obbligatoria a meno che sia **improbabile** che la violazione possa presentare **un rischio** per i diritti e le libertà delle persone;
- la comunicazione di una violazione alle persone fisiche diventa **necessaria** soltanto laddove la violazione possa **presentare un rischio elevato** per i diritti e le libertà delle persone fisiche**.**

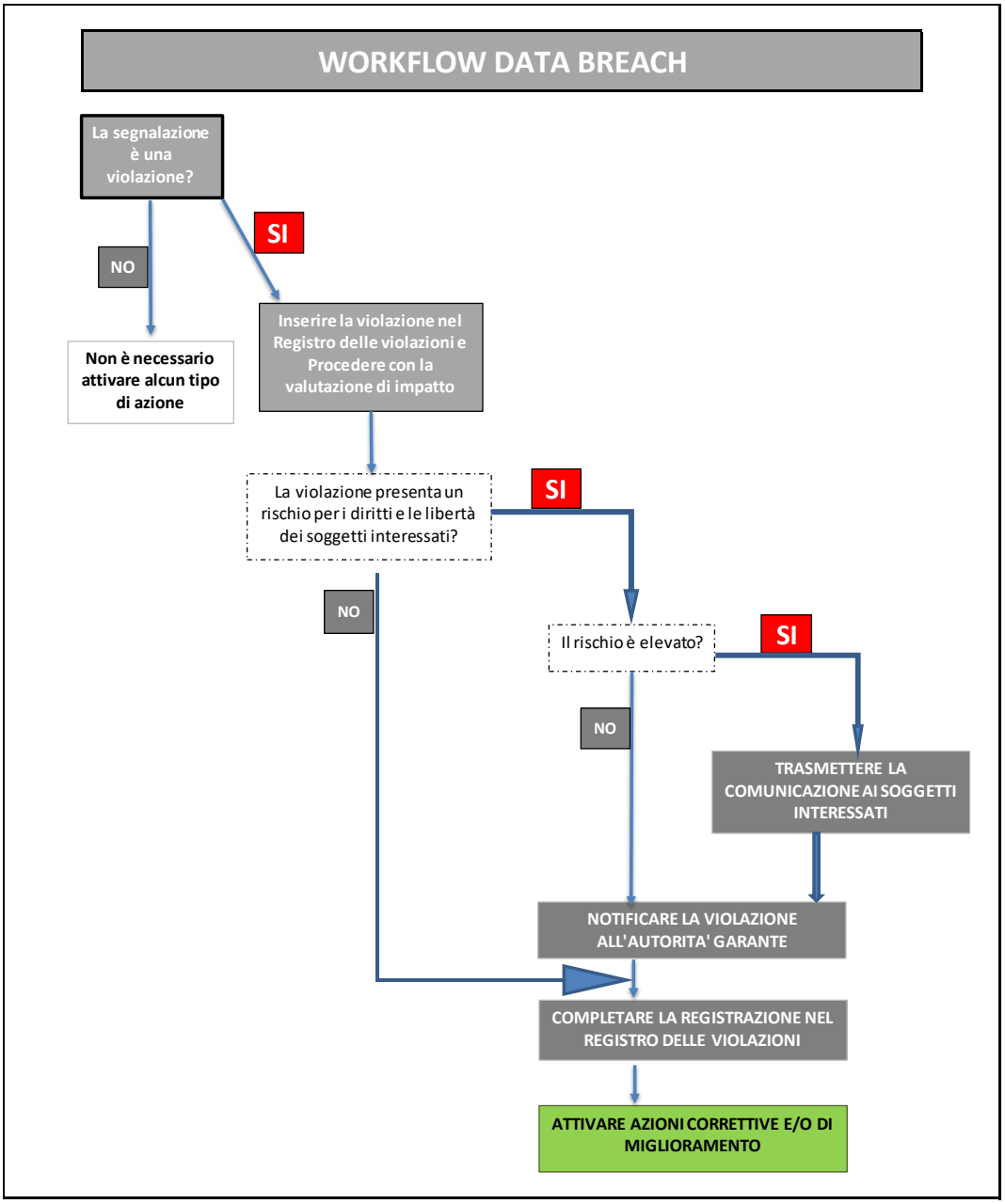
Ciò significa che non appena il Titolare del trattamento viene a conoscenza di una violazione, è fondamentale che non si limiti a contenere l'incidente, ma valuti anche il rischio che potrebbe derivarne. Questo per due motivi:

1. innanzitutto conoscere la probabilità e la potenziale gravità dell'impatto sulle persone fisiche aiuterà il Titolare del trattamento ad adottare misure efficaci per contenere e risolvere la violazione;
2. ciò lo aiuterà a stabilire se è necessaria la notifica all'autorità di controllo e, se necessario, alle persone fisiche interessate.

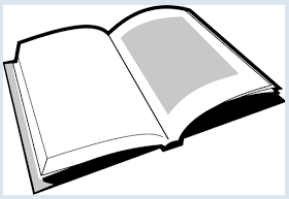
Come spiegato in precedenza negli steps della procedura, **la notifica di una violazione è obbligatoria a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche**, **mentre la comunicazione di una violazione agli interessati deve essere effettuata se è probabile che la violazione presenti un rischio *elevato* per i diritti e le libertà** delle persone fisiche. Tale rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati.
Esempi di tali danni sono la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie e il pregiudizio alla reputazione. Il verificarsi di tale danno dovrebbe essere considerato probabile quando la violazione riguarda dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza
Al fine di accertare la presenza o meno di rischio ai diritti e alle libertà dei soggetti interessati e determinarne il livello associato alla violazione subita, la tabella che segue riporta alcuni esempi:

LIVELLO DI IMPATTO	DESCRIZIONE
Nullo	I soggetti interessati/le persone fisiche non andranno incontro a nessun disagio.

Basso/Semplice	I soggetti interessati/le persone fisiche possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, ecc.). Ad es. la violazione interessa solo Dati Anagrafici (nomi, cognomi).
Medio	I soggetti interessati/le persone fisiche possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, ecc.).
Alto/Elevato	*Il trattamento può presentare rischi elevati per i diritti e le libertà delle persone fisiche.* I soggetti interessati/le persone fisiche possono andare incontro a conseguenze significative o addirittura irreversibili che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, ecc.).



6.2 Tipologia di violazione

ACCIDENTALI		VOLONTARI
Accesso non autorizzato		Accesso non autorizzato (SPIONAGGIO)
Copia non autorizzata		Copia non autorizzata (FURTO)
Divulgazione non prevista	**VIOLAZIONI**	Divulgazione non prevista (INFOTING)
Modifica non autorizzata		Modifica non autorizzata (IMPAIRMENT)
Perdita d'accesso	**6 X 2**	Perdita d'accesso (CIFRATURA/CRYPTOLOCK)
Cancellazione		Cancellazione (DISTRUZIONE)

ALCUNI ESEMPI

di violazioni che ricadono nell'art. 33

	CHIAVETTA USB (Persa)	FILE SYSTEM (cryptolocker)	E-MAIL (Invio errato)	ANTISPAM (diffusione)
ARCHIVI				
DATI	Excel con Nomi e cognomi dei clienti Prodotti acquistati	PDF e DOCX Tutti i documenti presenti sul file system compresi HR	E-mail: "La riunione di domani viene spostata alle 19" inviata ad altro collega	Tutti allegati di posta eletronica Registrati in DB per verifica

6.3 Analisi del rischio

Per poter procedere correttamente all'analisi della violazione occorre valutare adeguatamente il rischio associato ed il significato di:

- Riservatezza: stima del danno/impatto che la perdita di riservatezza riguardante l'asset comporterebbe per la tutela interessato
- Integrità: stima del danno/impatto che la perdita di integrità riguardante l'asset comporterebbe per la tutela interessato
- Disponibilità: stima del danno/impatto che la perdita di disponibilità riguardante l'asset comporterebbe per la tutela interessato

Per la valutazione della stima della perdita di Riservatezza, Integrità e Disponibilità viene utilizzata la seguente tabella.

Liv.	R- Riservatezza	I - Integrità	D- Disponibilità
1 - Basso	**Organizzazione** I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici. **Interessati** La mancanza di riservatezza ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. **Interessati** La mancanza di integrità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti. **Interessati** La mancanza di disponibilità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
2 - Medio	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti. **Interessati** La mancanza di disponibilità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

Liv.	R- Riservatezza	I - Integrità	D- Disponibilità
3 - Alto	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine) e un'eventuale loro diffusione ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti. **Interessati** La mancanza di **disponibilità** ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
4 - Critico	**Organizzazione** La diffusione delle informazioni ha elevati impatti sul business dell'organizzazione o sul rispetto della normativa vigente o sull'immagine dell'organizzazione tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** La mancanza di integrità delle informazioni ha elevati impatti sull' Istituto o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di integrità ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche. **Interessati** La mancanza di disponibilità ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

7. Comunicazione al Garante ed agli interessati

A seguito di un evento di Data Breach deve essere effettuata la comunicazione al Garante ed agli interessati. La comunicazione è coordinata dal Team Crisi. Le evidenze di tutte le comunicazioni debbono essere conservate.

7.1 Comunicazioni al Garante

Data breach, linee standard per la notifica delle violazioni di dati personali – il modello del Garante

Al fine di notificare la violazione dei dati personali all'autorità, è obbligatorio utilizzare procedura messa a disposizione dall'autorità stessa sul proprio sito al link https://www.garanteprivacy.it/data-breach

Si tratta di una procedura utilizzabile nel caso di "data breach", cioè la violazione della sicurezza privacy che obbliga tutti i Titolari del trattamento ad auto-segnalare l'incidente al Garante e alle persone potenzialmente danneggiate, a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone.

Come già detto, se il rischio è elevato, oltre alla notifica al Garante scatta anche l'obbligo di trasparenza a favore dei soggetti potenzialmente danneggiati. A questi due obblighi ci sono eccezioni, che vanno analiticamente giustificate già nel modello di notifica, che il Garante ha allegato al suo **provvedimento n. 157 del 30 luglio 2019**.

Gli obblighi, quando scattano, riguardano tutti coloro che trattando dati, senza esclusioni.

Di seguito si riporta quanto è opportuno indicare nel modello.

Tipo di notifica - La notifica al Garante potrebbe essere una notifica completa, oppure una notifica preliminare cui segue

una integrativa o più integrative.

Chi effettua la notifica - La notifica è un atto del Titolare del trattamento. Nella notifica, però, occorre indicare anche, se nominato, il DPO, responsabile della protezione dei dati, per informazioni relative alla violazione. Occorre anche segnalare ulteriori soggetti coinvolti nel trattamento, come i contitolari, i responsabili esterni del trattamento, i sub-responsabili e i rappresentanti del Titolare non stabilito nell'Ue.

I tempi - Le informazioni sintetiche sulla violazione riguardano, se accertato, il tempo della stessa (quando è avvenuta e se sia ancora in corso). Nel modello si chiede di indicare il momento (data e ora) in cui il Titolare del trattamento sia venuto a conoscenza della violazione. A questo proposito, rammentando che il regolamento Ue 2016/679 prevede un termine di **72 ore** (decorso il quale scattano sanzioni amministrative), il modello chiede di giustificare eventuali ragioni del ritardo. A corredo sono previste specificazioni a riguardo delle modalità con le quali il Titolare del trattamento è venuto a conoscenza della violazione, come per esempio notizie da parte del responsabile del trattamento, da parte di un interessato o da parte di terzi.

Il tipo di violazione - Ci sono tre tipi di violazioni: perdita di confidenzialità; perdita di integrità; perdita di disponibilità. Si deve indicare a quale appartenga la violazione.

È una violazione che tocca la **confidenzialità** quella che consiste in una diffusione o in un accesso non autorizzato o accidentale; riguarda, invece, la sfera della **integrità** una modifica non autorizzata o accidentale; concernono la **disponibilità** dei dati, infine, l'impossibilità di accesso, la perdita, distruzione non autorizzata o accidentale. La distinzione è importante ai fini della notifica analitica delle conseguenze della violazione.

Le conseguenze - In questa sezione si distinguono: conseguenze ed effetti negativi. Le conseguenze in caso di perdita di confidenzialità consistono in divulgazione eccessiva oppure nella possibilità di correlazione di dati oppure di utilizzo per finalità prima non previste. Le conseguenze in caso di perdita di integrità possono specificarsi nella modifica dei dati e/o della loro consistenza. Le conseguenze in caso di perdita di disponibilità possono attenere il mancato accesso a servizi, il malfunzionamento e difficoltà nell'utilizzo di servizi. In ogni campo del modello del Garante si lascia spazio a integrazioni relative ai singoli casi concreti.

Gli effetti - Nella sezione relativa agli effetti negativi per gli interessati, il compilatore deve indicare i potenziali danni, che possono attenere a danni economici, reputazionali, furti di identità, ecc. Si tratta di casistica anche qui non esaustiva, con possibilità di aggiunte specifiche.

La stima - Il modello chiede di prendere una posizione a riguardo della gravità della violazione, contrassegnando se la stessa sia trascurabile, bassa, media o alta, con le relative motivazioni.

Le cause - Si devono specificare le cause del data breach, da collegare ad azioni accidentali (interne o esterne) oppure ad azione intenzionale (interne o esterne).

Residua l'ipotesi, da dichiarare, di causa sconosciuta.

I dettagli - Il modello presenta spazi in cui discorsivamente e analiticamente descrivere l'incidente di sicurezza, le categorie di dati personali violati, i sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione e le misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture.

Dati personali - Il modello prevede una vasta casistica, non esaustiva, di dati oggetto di violazione: da quelli identificativi, ai recapiti fisici e virtuali, alle credenziali di accesso a internet o piattaforme, a comportamenti dell'interessati (navigazione internet), a dati di pagamento. Altre ipotesi riguardano i risultati di profilazione dell'interessato e l'intera serie dei dati sensibili, genetici e biometrici e i dati relativi a condanne e reati. Al compilatore è lasciata la possibilità di indicare qualsiasi altro dato, sebbene non elencato tra le varie opzioni espresse.

Quantità di dati - Il modello chiede di dare conto del volume, anche approssimativo, dei dati personali violati, oppure di indicare di non avere ancora una stima. In questa sezione si possono scrivere per esempio il numero di referti, il numero di record di un database, il numero di transazioni registrate.

Interessati - Fermo restando che coinvolti nella violazione la notifica non deve includere i dati personali oggetto di violazione e, tra essi, i nomi dei soggetti interessati dalla violazione, bisogna indicare le categorie.

Se ne ricordano alcune, precisando che l'elenco del modello non è esaustivo e il compilatore può aggiungere altre ipotesi: dipendenti, clienti, pazienti, minori, persone vulnerabili, ecc. Nel modello si chiede di indicare se è noto il numero preciso o stimato degli interessati.

Misure riparatorie - Nel modello si deve indicare quali misure riparatorie siano già state adottate o in corso di adozione

per diminuire i danni delle violazioni già subite e per prevenirne di future.

Comunicazione agli interessati - Il modello chiede di indicare se la violazione è stata comunicata agli interessati o sta per esserlo.

In caso negativo occorre spiegare al Garante la ragione di questa mancata comunicazione.

E' necessario essere convincenti e dettagliare per filo e per segno perché non è comunicato nulla agli interessati. Si ricordi che questo adempimento è quello che può compromettere la reputazione dell'impresa nei confronti dei propri clienti e, quindi, le eccezioni alla trasparenza devono essere attentamente vagliate.

In caso di comunicazione bisogna dettagliare il numero di interessati a cui è stata comunicata la violazione, il contenuto della stessa e il canale utilizzato (sms, posta cartacea o elettronica, altro da specificare).

Altre informazioni - Informazioni ulteriori riguardano l'eventuale segnalazione all'autorità giudiziaria o di polizia e gli eventuali coinvolgimenti di altri garanti, per esempio nel caso di interessati che si trovano nella Ue o fuori dello spazio economico europeo.

Per il fac-simile del modello, si veda modello inserito a sistema oppure https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501.

La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo **protocollo@pec.gpdp.it** oppure tramite posta elettronica ordinaria all'indirizzo **protocollo@gpdp.it** e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario. L'oggetto del messaggio deve contenere obbligatoriamente la dicitura **"NOTIFICA VIOLAZIONE DATI PERSONALI"** e opzionalmente la denominazione del titolare del trattamento.

7.2 Comunicazione agli interessati

La comunicazione agli interessati può avvenire con modalità diverse tra cui:

- comunicazione diretta agli interessati
- comunicato stampa
- comunicazione tramite sito WEB/social media
- altre forme

La comunicazione deve essere congruente con quanto accaduto.

Il Titolare, o suo delegato, definisce la strategia di *crisis communication* da mettere in atto da quando è a conoscenza durante dell'evento di Data Breach ed anche successivamente quando l'evento è stato risolto.

Di seguito le linee guida da considerare per la redazione delle comunicazioni verso gli interessati

Aspetti generali:

- definire il tono della comunicazione che può essere più informare (comunicato) o più formale (dichiarazione ufficiale)
- fornire un titolo "giornalistico" che per quanto possibile rassicuri gli interessati o perlomeno riducano il livello di allarme, utilizzare parole chiave facilmente rintracciabili sui motori di ricerca qualora venissero ricercate informazioni sui motori di ricerca
- le comunicazioni potrebbero non riguardare solo il Data Breach (rilevazione) ma anche le informazioni sull'andamento dello stesso nel tempo
- assicurare forme di comunicazione oneste, concrete e trasparenti
- fare riferimento al Titolare (ovvero Direzione o team dedicato), il suo ruolo ed il suo impegno
- mettere in evidenza la storia, l'impegno dell' Istituto nell'assicurare l'attenzione al tema, gli investimenti fatti, le misure applicate
- descrivere l'evento in modo facilmente comprensibile, quale impatto ha avuto sui dati (o quale impatto presumibile può avere – informazioni perse, violate, comunicate a terzi non autorizzati, diffuse, ecc), come lo si sta affrontando/è stato affrontato, specificare cosa l' Istituto sta facendo concretamente per proteggere i dati degli interessati
- indicare come e quando è stato coinvolto il Garante della Protezione dei dati
- inserire un contatto diretto per contattare l'organizzazione

- considerare di attivare un numero verde per rispondere agli interessati

Aspetti specifici per il comunicato stampa/dichiarazione ufficiale:

- prevedere link a pagina del sito web dove è reperibile ulteriore informazioni sul Data Breach ed anche lo stato dell'andamento dello stesso nel tempo

Aspetti specifici per la comunicazione tramite sito WEB/social media:

- Considerare di pubblicare (per le situazioni più gravi) anche un video di scuse/spiegazioni coinvolgendo il top management, affidarsi ad un esperto, qualora non si disponesse internamente di tali competenze, per evitare errori o creare più allarme del necessario
- considerare di attivare una APP dedicata all'evento

La comunicazione agli interessati deve contenere almeno i seguenti elementi:

Mittente:

Destinatario: [Nome e indirizzo dell'interessato colpito]

Introduzione…

In data [gg/mm/aaaa] abbiamo riscontrato una violazione dei suoi dati personali.

Come conseguenza della sopra menzionata violazione, i suoi dati personali potrebbero essere stati:

- Divulgati
- Distrutti
- Persi
- Modificati
- È stato eseguito l'accesso
- Altro [specificare]

da persone non autorizzate.

La informiamo che la violazione dei dati personali potrebbe avere le seguenti conseguenze: [elencare]

Per affrontare la violazione dei dati sono state/saranno implementate le seguenti misure:

Se avete quesiti in merito alla violazione dei dati, potete contattare [nome] via mail all'indirizzo […@....], o via posta all'indirizzo [indirizzo fisico].

La modalità di invio della comunicazione ed i riferimenti degli interessati coinvolti deve essere riportata nel MODULO Gestione del Data Breach Sezione 7

7.3 Comunicazione all'Organo di governo all' Istituto

A seguito di un evento che ricade nei casi 4 e 5, ed in ogni caso qualora il Titolare del trattamento lo ritenesse opportuno, deve essere tenuto aggiornato l'Organo di governo dell' Istituto. Tale attività è a cura del Titolare del trattamento e deve avvenire con modalità, per quanto possibili rintracciabili.

8. Situazioni anomale o di emergenza

In caso di segnalazioni in situazioni anomale o di emergenza, quali:

- mancanza di figure apicali
- mancanza di collegamenti (es. internet)/energia/situazioni di emergenza dovute a cause di forza maggiore)

Devono essere considerate le seguenti misure:

- Le riunioni del Titolare o Team dedicato possono essere effettuate in luoghi diversi dalla sede dell' Istituto ed eventualmente con strumenti quali skype, ecc

11.ALLEGATO N. 4 - DATA BREACH REGISTRO DELLE VIOLAZIONI

REGISTRO DELLE VIOLAZIONI (DATA BREACH)

Progr.	Data	Evento	Descrizione conseguenze	Livello di RISCHIO	Descrizione provvedimenti adottati	Notifica ad Autorità di Controllo		Comunicazione all'interessato	
						SI/NO	Data	SI/NO	Data
1									
2									

Note per la compilazione

Il presente registro deve essere compilato e aggiornato ogniqualvolta si manifesti una violazione dei dati personali, al fine di rendicontare e monitorare la corretta esecuzione delle attività.

Di seguito le modalità operative:

Colonna A - Data:

indicare la data dell'evento oppure la data in sui si viene a conoscenza della violazione.

Colonna B - Evento:

selezionare la tipologia di evento occorso:

Classificazione evento
DISTRUZIONE di dati illecita
PERDITA di dati illecita
MODIFICA di dati illecita
DISTRUZIONE di dati accidentale
PERDITA di dati accidentale
MODIFICA di dati accidentale
DIVULGAZIONE non autorizzata
ACCESSO ai dati personali illecito

Colonna C - Descrizione conseguenze:

inserire la descrizione generale dell'evento occorso (legato alla tipologia di evento selezionato nella colonna B) e l'ambito di interesse (inserire una descrizione in sintesi oppure semplice rimando all'ALLEGATO M1 compilato della Procedura di Gestione delle Violazioni)

Colonna D - Livello di Rischio:

sulla base dell'evento occorso, determinare il livello di rischio:

Rischio
Nullo
Basso
Medio
Elevato

Per la corretta determinazione si veda quanto esposto nell'ALLEGATO M2 - modello di valutazione del rischio connesso al data breach della Procedura di Gestione delle Violazioni

Colonna E - Descrizione provvedimenti adottati:

inserire breve descrizione delle misure adottate per il contenimento della violazione

Colonna F/G - Notifica ad Autorità di controllo:

(di monitoraggio attività) per livelli di rischio basso/ medio /alto è necessaria la comunicazione al Garante, mentre non sarà necessaria in caso di rischio "nullo"

Colonna H - Comunicazione all'Interessato:

(di monitoraggio) sarà uguale a “Sì” solo per violazioni di livello elevato

12.ALLEGATO N. 5 – DATA BREACH - FORM PER LA RACCOLTA INFORMAZIONI

1. luogo e data dell'evento (anche approssimativi se non sono noti):

_____

2. breve descrizione dell'evento:

_____

_____

3. indicazione dei trattamenti di dati coinvolti (riportare elenco dei trattamenti?)

_____

_____

4. banche dati o archivi anche cartacei che sono stati violati:

_____

_____

5. tipo di violazione

☐lettura (presumibilmente i dati non sono stati copiati)

☐copia (i dati sono ancora presenti sul sistema del titolare)

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

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

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

☐altro: _____

6. Dispositivo oggetto della violazione

☐Computer ☐Dispositivo mobile

☐Rete ☐File o parte di un file

☐Strumento di backup ☐Documento cartaceo

☐Altro: _____

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

_____

_____

8. Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

☐N. _____persone ☐Circa _____persone

☐Un numero (ancora) sconosciuto di persone

9. Che tipo di dati sono oggetto di violazione?

☐Dati anagrafici/codice fiscale ☐Dati relativi a minori

☐Dati di accesso e di identificazione (username, password, customer ID, altro)

☐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

13. ALLEGATO N. 6 – DATA BREACH - MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

Assessment di gravità	A cura del Titolare del trattamento e/o suo delegato, del Referente Privacy, del Tecnico Informatico (e del DPO, qualora nominato)
Dispositivi oggetto del Data Breach (computer, rete dispositivo mobile, file o parte di un file, strumento di back-up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): - lettura (presumibilmente i dati non sono stati copiati), - copia (i dati sono ancora presenti sui sistemi del Titolare), - alterazione (i dati sono presenti sui sistemi ma sono stati alterati), - cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), - furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione), - altro_____.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.	
Se laptop/pc/tablet è stato perso/rubato: quando è stata l'ultima volta in cui il laptop/pc/tablet è stato sincronizzato con il sistema informatico centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
Su quale **settore aziendale**, la violazione ha avuto conseguenze negative?	
Qual è la **natura dei dati coinvolti**? Compilare le sezioni sottostanti:	
• I **dati particolari** (come identificati dall'artt 9-10 del Regolamento), relativi ad una persona viva ed individuabile: a) origine razziale o etnica; b) opinioni politiche, convinzioni religiose o filosofiche; c) appartenenza sindacale; d) dati genetici; e) dati biometrici giudiziari; f) relativi alla salute o orientamento sessuale di una persona.	
• **Informazioni che possono essere utilizzate per commettere furti di identità** (ad es. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito);	
• **Informazioni personali relative a soggetti fragili** (ad es. anziani, disabili, minori);	

Assessment di gravità	A cura del Titolare del trattamento e/o suo delegato, del Referente Privacy, del Tecnico Informatico (e del DPO, qualora nominato)
• Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone;	
Altro:	
La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? (ad es. la pseudonimizzzione e la cifratura dei dati personali)	
Il Titolare del trattamento ha aderito ad un codice di condotta approvato ai sensi dell'art. 40 del Regolamento o un meccanismo di certificazione di cui all'art. 42 del Regolamento?	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della violazione: **1. Rischio nullo** **2. Rischio semplice/basso** **3. Rischio medio** **4. Rischio elevato/alto**	
Notificazione del Data Breach all'Autorità Garante	☐ **SI** ☐ **No** **Se si, notificato in data:** **Dettagli:**
Comunicazione del Data Breach agli interessati (solo in caso di rischio elevato)	☐ **SI** ☐ **No** **Se si, notificato in data:** **Dettagli:**
Compilatore	
data	

14.ALLEGATO N. 7 – PROCEDURA DI RISCONTRO AI DIRITTI DELL'INTERESSATO

Allo scopo di adempiere compiutamente agli obblighi incombenti sul Titolare ai sensi e per gli effetti degli artt. 12 ss Reg.UE 2016/679, l' Istituto ha elaborato la presente procedura volta a rendere edotte le funzioni aziendali preposte al trattamento dei dati delle modalità e dei termini di riscontro delle istanze formulate dagli interessati.

1. Soggetto preposto al riscontro delle istanze dell'interessato

Il Titolare ha affidato al DPO il compito di riscontrare, per iscritto, le istanze formulate dall'interessato.

2. Modalità ed oggetto della richiesta di informazioni

L'interessato deve inoltrare la propria istanza attraverso il canale di contatto indicato nell'informativa al trattamento dei dati personali. Ai sensi degli artt. 15 ss. Del Reg. UE 2016/679 l'Interessato può esercitare i seguenti diritti, alle condizioni di seguito indicate:

a) diritto di accesso, richiedendo conferma o meno del trattamento di propri dati personali ed informazioni relative all'origine dei dati, alle finalità, alle modalità ed alla durata del trattamento, ai soggetti terzi ai quali i dati vengono trasmessi, all'esistenza di un processo decisionale automatizzato.

b) diritto di rettifica, qualora i dati dell'interessato risultino inesatti o incompleti.

c) diritto di cancellazione: si precisa come tale diritto possa essere legittimamente esercitato qualora i) i dati non siano più necessari rispetto alle finalità per i quali sono stati raccolti; ii) l'interessato abbia revocato il proprio consenso al trattamento dei dati (nel caso il cui il trattamento sia basato sul consenso); iii) l'interessato si opponga al trattamento; iv) i dati siano trattati illecitamente; v) la cancellazione dei dati sia imposta da un obbligo legale; vi) il trattamento è relativo a dati personali relativi ad un minore di anni 16 e non è stato autorizzato dal titolare della responsabilità genitoriale.

d) diritto di limitazione del trattamento: si precisa come tale diritto possa essere esercitato nella misura in cui l'interessato: i) contesti l'esattezza dei propri dati, in tale caso il Responsabile dovrà limitare il trattamento per il periodo necessario a valutare la fondatezza delle contestazioni mosse dall'interessato; ii) i dati siano trattati illecitamente; iii) i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

e) diritto alla portabilità dei dati: l'interessato ha diritto di ricevere i propri dati, in un formato strutturato di uso comune e leggibile da dispositivo automatico, ed ha diritto di richiedere la trasmissione di tali dati ad altro Titolare. Si precisa come il diritto in esame sia esercitabile unicamente nel caso in cui il trattamento sia basato sul consenso dell'interessato o sull'esecuzione di un contratto di cui lo stesso è parte contraente ed il trattamento sia effettuato con mezzi automatizzati.

3. Verifica dell'identità dell'interessato

il Referente Privacy, prima di procedere al riscontro, può richiedere all'interessato di fornire prova della propria identità qualora nutra ragionevoli dubbi circa l'identità dell'Interessato.

4. Modalità e termini di riscontro

L'istanza dell'interessato deve essere riscontrata dal Referente Privacy, per iscritto, senza ingiustificato ritardo entro e non oltre un mese dal ricevimento della stessa, fornendo le informazioni richieste in un formato strutturato di uso comune, salvo diversa indicazione dell'interessato medesimo.

Il termine indicato può essere prorogato di due mesi, se necessario, in ragione della complessità dell'istanza o dell'elevato numero delle richieste. In tale ultima ipotesi il Referente Privacy è tenuto a indicare, nel riscontro, le motivazioni che giustificano il mancato rispetto del termine di un mese.

5. Ipotesi di diniego e limitazione ai diritti dell'interessato (D.lgs 101/2018)

Il Referente Privacy può rifiutare di soddisfare l'istanza qualora, non possa essere stabilita l'identità dell'interessato ovvero qualora la richiesta risulti

i) illegittima, ovvero non rientri tra i diritti esercitabili dall'interessato di cui al precedente p.to 2;

ii) manifestamente infondata o eccessiva, ovvero la stessa richiesta sia sta reiterata, più volte, a breve distanza di tempo. In tale ultimo caso, il responsabile può addebitare all'interessato un contributo spese ragionevole. Al di fuori di tale ipotesi il riscontro non può comportare oneri e spese a carico dell'interessato;

I diritti di cui al precedente p.to 2 (Artt. 15-22 Reg.UE 2016/679) non possono esercitati dall'interessato qualora dall'esercizio di tali diritti possa derivare un pregiudizio:

1. agli interessi tutelati in base alle disposizioni in materia di antiriciclaggio ed in materia di sostegno alle vittime di richieste estorsive;
2. allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;
3. all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'art. 82 della Costituzione;
4. alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
5. alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio

6. Notifica ai Responsabili del Trattamento

Qualora il Referente Privacy dia seguito ad una istanza di rettifica, cancellazione dei dati o limitazione del trattamento, lo stesso è tenuto a comunicare l'avvenuta rettifica, cancellazione dei dati o limitazione del trattamento ai terzi Responsabili del Trattamento ai quali i dati sono stati trasmessi, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Qualora ricorra tale ultima ipotesi, il Referente Privacy è tenuto ad informare prontamente il Titolare delle motivazioni dell'omessa comunicazione ai Responsabili del Trattamento.

15.ALLEGATO N. 8– MODULO ESERCIZIO DIRITTI DELL'INTERESSATO

All'attenzione di[1]
(indicare il titolare del trattamento)

ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a…….
nato/a a……il……, esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali

(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto *(barrare solo le caselle che interessano)*:

- ☐ chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
- ☐ in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni previste alle lettere da a) a h) dell'art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;
  - le finalità del trattamento;
  - le categorie di dati personali trattate;
  - i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
  - il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
  - l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
  - l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Richiesta di intervento sui dati

(artt. 16-18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

- ☐ rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);
- ☐ cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

  a)…;

  b)….;

  c)…;

[1] Indirizzare al titolare del trattamento (ad esempio: banche, operatori telefonici, sistemi di informazioni creditizie, gestori di siti web, assicurazioni, strutture sanitarie, pubbliche amministrazioni, etc.), anche per il tramite del Responsabile della Protezione dei Dati (RPD), ove designato dal titolare.

nei casi previsti all'art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l'attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell'interessato di cancellare link, copie o riproduzioni dei suoi dati personali;

☐ limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:

- ☐ contesta l'esattezza dei dati personali;
- ☐ il trattamento dei dati è illecito;
- ☐ i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- ☐ l'interessato si è opposto al trattamento dei dati ai sensi dell'art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

3.Portabilità dei dati[2]

(art. 20 del Regolamento (UE) 2016/679)

Con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

☐ ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;

☐ trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare: ……..):*

- ☐ tutti i dati personali forniti al titolare;
- ☐ un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____
_____
_____
_____
_____
_____
_____
_____
_____

4. Opposizione al trattamento

(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

[2] Per approfondimenti: Linee-guida sul diritto alla "portabilità dei dati" - WP242, adottate dal Gruppo di lavoro Art. 29, disponibili in www.garanteprivacy.it/regolamentoue/portabilita.

☐ Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell'art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____
_____
_____
_____
_____
_____

5. Opposizione al trattamento per fini di marketing diretto

(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

☐ Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

_____

Il sottoscritto:

☐ Chiede di essere informato, ai sensi dell'art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.

☐ Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell'art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

_____

Recapito per la risposta[3]:

Via/Piazza
Comune Provincia Codice postale

oppure

e-mail/PEC:

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

_____
_____
_____

[3] Allegare copia di un documento di riconoscimento

_____
_____
_____
_____
_____

(Luogo e data)

(Firma)