MODELLO DI

ORGANIZZAZIONE

E GESTIONE DELLA PRIVACY

EX REGOLAMENTO UE

679/2016

ALIPLAST

Società del Gruppo Herambiente

M170 rev.03 del 30.06.2020

A seguito di analisi della struttura aziendale il documento fornisce idonee informazioni riguardanti:

1 PREMESSE

Il Regolamento Europeo 679/2018 divenuto cogente dal 25.05.2018 ha introdotto una normativa europea omogenea in materia di protezione e libera circolazione dei dati personali. La nuova normativa si affianca con efficacia di fonte di diritto di rango superiore al Codice della Privacy ovvero la legge 196/2003 così come modificata dal Dlgs. 101/2018, determinando fondamentalmente il passaggio dalle misure minime di protezione del dato personale alle cosiddette misure adeguate alla singola organizzazione. Il decreto di coordinamento, per cui è stata data delega al Governo, ha in ogni caso salvato tutti i provvedimenti generali del garante in quanto compatibili. Tanto premesso, la società si è conformata al cosiddetto principio di accountability (responsabilizzazione), suggellato dal Regolamento, adottando un proprio modello di organizzazione e gestione della privacy che si è articolato nelle seguenti fasi:

- Fase 1 – Valutazione della compliance: raccolta di tutte le informazioni sull'organizzazione aziendale, analisi e valutazione della documentazione in uso;
- Fase 2 – Creazione del registro dei trattamenti: documento volto a tenere traccia dei trattamenti effettuati da parte del titolare e degli eventuali responsabili, e contenente, tra gli altri, le finalità del trattamento, una descrizione delle categorie di interessati e dei dati personali, i destinatari, gli eventuali trasferimenti verso Paesi terzi e una descrizione generale delle misure di sicurezza;
- Fase 3 – Stesura/Modifica della documentazione affinché risulti completa ed aggiornata secondo le prescrizioni della nuova normativa;
- Fase 4 – Individuazione dei ruoli e delle responsabilità dei soggetti che effettuano il trattamento;
- Fase 5 – Definizione delle politiche di sicurezza e valutazione dei rischi: valutazione e attuazione di tutte le misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. Questa fase è espressione, soprattutto, del principio di responsabilizzazione del titolare (accountability);
- Fase 6 – Processo di Data Breach: al fine di assicurarsi di aver adottato tutte le procedure idonee a scoprire eventuali violazioni, previsione di adeguata reportistica nella quale indicare le cause nonché gli effetti della violazione subita;
- Fase 7 – Valutazione d'impatto sulla protezione dei dati personali: al fine di assicurare trasparenza nelle operazioni di trattamento dei dati personali e adeguata protezione agli stessi, implica che il titolare effettui precise e adeguate valutazioni d'impatto privacy. Attraverso tale istituto è possibile, quindi, valutare gli aspetti relativi alla protezione dei dati, prima che questi vengano trattati. Il titolare è inoltre tenuto ad applicare nell'organizzazione i principi della privacy by design nel senso di valutare gli aspetti della privacy a partire dallo stesso concepimento di un nuovo processo produttivo e della privacy by default ovvero settare tutti i processi aziendali nella direzione delle limitazioni e minimizzazione dei trattamenti;
- Fase 8 – Implementazione dei processi per l'esercizio dei diritti dell'interessato;
- Fase 9 – Formazione del personale in ordine agli aspetti della privacy;
- Fase 10 Si è valutata la possibilità di nominare un Responsabile della Protezione dei dati, ma, alla luce delle linee guida del WP 29, è stato ritenuto non necessario in considerazione della tipologia di dati trattati e del contesto in cui opera l'azienda.

2 CATEGORIE DI DATI PERSONALI TRATTATI IN ALIPLAST SPA

A seguito dell'analisi compiuta si sono identificate le seguenti categorie di dati personali:

- DATI COMUNI RELATIVI AL PERSONALE O AI CANDIDATI PER DIVENTARLO, DI NATURA ANCHE "PARTICOLARE"
- DATI COMUNI RELATIVI AI CLIENTI
- DATI COMUNI RELATIVI AI FORNITORI

- DATI ANCHE "PARTICOLARI" INDISPENSABILI ALLO SVOLGIMENTO DELL'ATTIVITÀ LAVORATIVA PER ASSOLVERE OBBLIGHI NORMATIVI E CONTRATTUALI

2.1 Liceità del trattamento

Le basi giuridiche del trattamento cioè i presupposti giuridici del trattamento ai sensi dell'art.6 del GDPR 679/2016 sono:

- L'interesse vitale dell'individuo
- L'interesse pubblico
- L'esigenza contrattuale
- La conformità ad obblighi legali
- Il consenso non ambiguo dell'individuo
- L'interesse legittimo del titolare del trattamento.

Nel caso della società ALIPLAST quasi tutti i trattamenti sono effettuati sulla base di *obblighi legali* o *contrattuali*.

Tanto premesso Il trattamento dei dati in ALIPLAST è effettuato attraverso strumenti automatizzati e non, in conformità alle finalità indicate e nel rispetto dei requisiti di riservatezza e delle più idonee misure di sicurezza.

Ai sensi di quanto previsto dall'art. 5 del GDPR 679/2016, i dati personali devono essere trattati:

- in modo lecito, corretto e trasparente;
- raccolti per finalità determinate esplicite e legittime
- successivamente trattati in modo coerente con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati;
- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione degli interessati;
- in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

3 SEDI DEL TRATTAMENTO

Il trattamento dei dati avviene, oltre che nella sede principale di Istrana, in Via delle Fornaci n. 14, anche nelle sedi operative periferiche di:

- Gualdo Cattaneo (PG), frazione di S. Terenziano, in via dell'Artigianato n.13;
- Formigine (MO), in via Quattro Passi n.108;
- Quinto di Treviso (TV), in via Enrico §Mattei n.92.

4 ANALISI DEI RISCHI CUI SONO SOGGETTI I DATI

L'identificazione e la valutazione degli aspetti connessi ai rischi derivanti dal trattamento dei dati personali sono regolati nella procedura di gruppo P163 "valutazione di impatto dei trattamenti sulla protezione dei dati personali".

4.1 Strumenti impiegati nel trattamento

Sono stati individuati come sorgenti soggette a rischio le seguenti categorie di strumenti utilizzati per il trattamento:

Strumenti	Legenda
Schedari e altri supporti custoditi nell'area controllata	*A*
Elaboratori in rete privata custoditi nell'area controllata	*B*
Elaboratori in rete pubblica (internet) nell'area controllata	*C*

Fattori di rischio	Basso	Medio	Elevato
Rischio d'area legato all'accesso non autorizzato nei locali	*A B C*		
Rischio guasti tecnici hardware, software, supporti		*B C*	
Rischio penetrazione nelle reti di comunicazione	*B C*		
Rischio legato a errori umani		*A B C*	
Rischio d'area per possibili eventi distruttivi	*A B C*		

4.2 Valutazione dei rischi per singoli trattamenti

I criteri di valutazione dei rischi, la valutazione dei rating di rischio e i risultati dell'analisi dei singoli trattamenti sono definiti su "Gestione rischi e opportunità" P22, a cui si rimanda.
I risultati di tale analisi dei rischi sono registrati su "…" RXXX.

[…omissis…]

5 DISTRIBUZIONE COMPITI E RESPONSABILITÀ

5.1 "Titolare" del Trattamento dei dati

Per il trattamento dei dati personali il titolare, identificato nella figura dell'amministratore delegato, ha nominato un suo rappresentante sul quale ricade la responsabilità di determinare le finalità ed i mezzi del trattamento dei dati personali.

5.2 "Responsabile" del Trattamento dei dati dell'unità organizzativa (RUO)

Il titolare del trattamento dati agisce, oltre che attraverso il suo rappresentante, servendosi di direttori e responsabili di funzione che ricoprono il ruolo di "responsabili trattamento dati dell'unità operativa (RUO)" nella misura in cui svolgono tutti i compiti che la normativa di riferimento prescrive ad Aliplast relativamente al trattamento dei dati personali effettuati nell'ambito o per conto dell'unità organizzativa di appartenenza, coordinando la loro attività anche in rapporto alle linee guida definite dalla Direzione QSA di gruppo. Il rappresentante del titolare (5.1) viene definito come RUO di I° livello mentre gli altri responsabili sono da intendersi come RUO di II° livello.

5.3 Soggetti "Autorizzati" al Trattamento dei dati

Il trattamento dei dati personali particolari viene effettuato solo da soggetti che hanno ricevuto un formale incarico per iscritto di ogni singolo incarico, con il quale s'individua l'ambito del trattamento consentito.
Le lettere di incarico che vanno a completare il mansionario sono allegate al presente documento.

5.4 Formazione dei "soggetti autorizzati" al trattamento

Il titolare fornisce direttamente agli incaricati al trattamento la necessaria formazione:

- al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansione;

- in occasione dell'introduzione di nuovi strumenti e programmi informatici.
- In occasione dell'introduzione di nuove normative aventi impatto sulla privacy.

La formazione interesserà sia le norme generali in materia di privacy sia gli aspetti peculiari dei trattamenti effettuati.

6 SEDE PRINCIPALE DI ISTRANA (TV)

6.1 Aree, locali e strumenti con i quali si effettuano i trattamenti

Gli uffici sono dislocati al piano terra e fanno parte dello stesso stabilimento in cui è sita anche l'area produttiva. Il complesso immobiliare è controllato da telecamere di videosorveglianza regolarmente autorizzate dall'ispettorato del lavoro.
Le porte d'ingresso si presentano con chiavi di sicurezza.
La sede aziendale è altresì dotata di sistema d'allarme del tipo elettronico con sensori di tipo volumetrico.
L'accesso all'immobile è controllato da portone d'ingresso con citofono e suoneria d'ingresso.
Tutti gli accessi all'area ufficio di personale non dipendente sono registrati su supporto cartaceo.

6.2 Schedari e altri supporti cartacei

I supporti cartacei, contenenti dati sensibili sono raccolti in raccoglitori custoditi in armadiature chiuse a chiave.

6.3 Elaboratori in rete privata

Il sistema di lavoro della struttura avviene con elaborazione in rete privata ethernet. Si dispone di una rete di lavoro realizzata mediante collegamenti via cavo costituita da:

- N **3** server fisici dotato di dischi raid (vmware)
- N **1** firewall hardware
- N **4** nas
- N **1** gruppo di continuità dedicato a uffici
- N **33** stampanti/ fotocopiatrici e MFP, in area ufficio
- N **16** virtual server
- N **5** access point wireless
- N **66** postazioni di lavoro in area ufficio
- N **10** gruppi di continuità in area produttiva

6.4 Elaboratori in rete pubblica (internet)

Sono collegati a internet i seguenti computer:

- N **66** postazioni di lavoro dislocate nell'area ufficio;
- N **7-10** postazioni dislocate nell'area produttiva (solo per teleassistenza).

Protezione del Sistema mediante:

- ESET ANTIVIRUS NOD32

Tipologia di software caricati sui PC:

Id Produttore	Nome Software	Versione
7ZIP	7ZIP	
ACRONIS	BACKUP & RECOVERY	10
ACRONIS	BACKUP FOR VMWARE	9
ADOBE	CREATIVE SUITE DESIGN	4 PREMIUM
ADOBE	READER	DC 18
AUTODESK	AUTOCAD	2008 LT
AUTODESK	AUTOCAD	2016 LT
BUSINESS	BUSINESS	ND
DANEA	EASYFATT	2006
DEVCOMPONENTS	DOTNETBAR WIN FORM	12.9.02

DIESSE	ECO EXPERT	ND
DISPLAY FUSION	DISPLAY FUSION	6.1
ECOS	BASE	ND
ECOS	MODULO	STOCCAGGIO
ESET	NOD32	6.6
IPERIUS	BACKUP	ND
MAILSTORE	MAILSTORE	10
MDAEMON	MDAEMON SERVER	18.0
MICROSOFT	NAVISION	5.0 SP1
MICROSOFT	OFFICE	XP PRO
MICROSOFT	OFFICE	2007
MICROSOFT	OFFICE	2013 STD OPEN
MICROSOFT	SQL SERVER	2014
MICROSOFT	VISIO	2007 STD
MICROSOFT	VISIO	2010 STD
MICROSOFT	VISUAL STUDIO	2012 PRO
SNARE	LOG_COLLECTOR	ND
OBVIOUS IDEA	LIGHT IMAGE RESIZER	ND
PROGESOFT	INTELLICAD	2002
PROGESOFT	PROGECAD	2006
SIELCO SISTEMI	WINLOG	256 TAG W-NET/I-USB+
SIELCO SISTEMI	WINLOG	64 TAG W-E/S-USB+
SIELCO SISTEMI	WINLOG	128 TAG W-E/S
SUPREMO	SUPREMO RDP ESKTOP	
TEAMVIEWER	TEAMVIEWER	
TSPLUS	TSPLUS	
XLINE	PHP RUNNER	9.8
ZUCCHETTI	MICROFOCUS	ND

Backup eseguiti con frequenza:

- 1 volta al giorno per dati utenti, cartelle di rete e database gestionale, di notte su nas,
- 1 volta al giorno per dati utenti, cartelle di rete e database gestionale, di mattina su cassette rdx

PC collegati mediante:

- Dominio in Area Uffici,
- Workgroup in Area Produttiva.

6.5 Piattaforme che utilizzano tecnologia web

- Sito internet aziendale

6.6 Mappa dei trattamenti effettuati

Dal riepilogo dei dati trattati, così come risulta anche nel registro dei trattamenti di cui all'art. 30 GDPR, che si allega al presente modello e dall'identificazione degli strumenti utilizzati si delinea il seguente schema:

Tipologia trattamento	*Cartaceo*	*Computer non in rete*	*Computer in rete privata*	*Computer in rete pubblica*	*Video sorveglianza*
Dati comuni relativi a clienti /fornitori	**X**		**X**		**X**
Dati comuni relativi a lavoratori	**X**		**X**		**X**
Dati relativi allo svolgimento di attività economiche/ commerciali	**X**		**X**		
Dati di natura giudiziaria dei lavoratori	**X**				

Dati idonei a rilevare lo stato di salute dei lavoratori	X		X		

6.7 Analisi dei trattamenti effettuati

Dalla rilevazione degli strumenti utilizzati e delle tipologie dei dati trattati emerge che:

- i dati personali vengono sistematicamente trattati con supporti cartacei e con elaborazione;
- i dati "particolari" trattati con elaborazione sono limitati a quelli necessari ad assolvere agli obblighi normativi e contrattuali con riferimento alla materia giuslavoristica; trattasi dei soli dati del personale dipendente;
- gli elaboratori in rete pubblica presenti dispongono esclusivamente del collegamento a internet.

7 SEDE OPERATIVE PERIFERICHE

7.1 Sede di Gualdo Cattaneo (PG)

7.1.1 Aree, locali e strumenti con i quali si effettuano i trattamenti

Gli uffici tecnici e amministrativi sono dislocati al piano terra dello stesso stabilimento in cui è sita anche l'area produttiva, mentre quelli direzionali si trovano al primo piano dello stesso edificio. Esiste un altro edificio posizionato difronte a quello direzionale/produttivo, che funge da magazzino sia per le materie prime che per il prodotto finito. Entrambe le sedi sono dotate di sistema d'allarme del tipo elettronico con sensori di tipo volumetrico. L'accesso all'immobile è controllato da portone d'ingresso con citofono e suoneria d'ingresso.
Le porte d'ingresso si presentano con chiavi di sicurezza.

7.1.2 Schedari e altri supporti cartacei

I supporti cartacei, contenenti dati sensibili sono raccolti in raccoglitori custoditi in armadiature chiuse a chiave.

7.1.3 Elaboratori in rete privata

Il sistema di lavoro della struttura avviene con elaborazione in rete privata ethernet. Si dispone di una rete di lavoro realizzata mediante collegamenti via cavo costituita da:

- N **1** server fisico dotato di dischi raid (vmware)
- N **2** virtual servers
- N **1** router con access point wireless
- N **7** postazioni di lavoro in area ufficio
- N **4** postazioni di lavoro in area produttiva
- N **2** stampanti/ fotocopiatrici MFP
- N **1** fax
- N **1** switch di rete

7.1.4 Elaboratori in rete pubblica (internet)

Sono collegati a internet i seguenti computer:

- N **7** postazioni di lavoro dislocate nell'area ufficio;
- N **4** postazioni dislocate nell'area produttiva.

Protezione del Sistema mediante:

- ESET ANTIVIRUS NOD32

Tipologia di software caricati sui PC:

Id Produttore	Nome Software	Versione
7ZIP	7ZIP	VARIA
TEAMSYSTEM	GAMMA ENTERPRISE	ND
TEAMSYSTEM	SOFTWARE TIME	ND
NANOSYSTEMS SRL	SUPREMO RDP DESKTOP	VARIA
ADOBE	READER	VARIA
MICROSOFT	OFFICE	XP PRO / 2007 / 2013
MICROSOFT	SQL SERVER	2003
MICROSOFT	NAVISION	5.0 SP1
ECOS	ECOS BASE	WEB

Backup eseguiti con frequenza:

- 1 volta al giorno per dati utenti, cartelle di rete e database gestionale, di notte su cassette rdx

PC collegati mediante:

- Dominio in Area Uffici,

7.1.5 Piattaforme che utilizzano tecnologia web

- Nessuna

7.1.6 Mappa dei trattamenti effettuati

Dal riepilogo dei dati trattati, così come risulta anche nel registro dei trattamenti di cui all'art. 30 GDPR, che si allega al presente modello e dall'identificazione degli strumenti utilizzati si delinea il seguente schema:

Tipologia trattamento	*Cartaceo*	*Computer non in rete*	*Computer in rete privata*	*Computer in rete pubblica*	*Video sorveglianza*
Dati comuni relativi a clienti /fornitori	X		X		
Dati comuni relativi a lavoratori	X		X		
Dati relativi allo svolgimento di attività economiche/ commerciali	X		X		
Dati di natura giudiziaria dei lavoratori	X				
Dati idonei a rilevare lo stato di salute dei lavoratori	X		X		

7.1.7 Analisi dei trattamenti effettuati

Dalla rilevazione degli strumenti utilizzati e delle tipologie dei dati trattati emerge che:

- i dati personali vengono sistematicamente trattati con supporti cartacei e con elaborazione;
- i dati "particolari" trattati con elaborazione sono limitati a quelli necessari ad assolvere agli obblighi normativi e contrattuali con riferimento alla materia giuslavoristica; trattasi dei soli dati del personale dipendente;
- gli elaboratori in rete pubblica presenti dispongono esclusivamente del collegamento a internet.

7.2 Sede di Formigine (MO)

7.2.1 Aree, locali e strumenti con i quali si effettuano i trattamenti

Gli uffici sono dislocati al primo piano dello stesso stabilimento in cui è sita anche l'area arrivo e scarico rifiuti, mentre la parte produttiva e di stoccaggio prodotto finito è in uno stabilimento adiacente. Il complesso immobiliare è controllato da telecamere di videosorveglianza regolarmente autorizzate dai Sindacati.
Le porte d'ingresso si presentano con chiavi di sicurezza.
La sede aziendale è altresì dotata di sistema d'allarme del tipo elettronico con sensori di tipo volumetrico.
L'accesso all'immobile è controllato da portone d'ingresso con citofono e suoneria d'ingresso.

7.2.2 Schedari e altri supporti cartacei

I supporti cartacei, contenenti dati sensibili sono raccolti in raccoglitori custoditi in armadiature chiuse a chiave.

7.2.3 Elaboratori in rete privata

Il sistema di lavoro della struttura avviene con elaborazione in rete privata ethernet. Si dispone di una rete di lavoro realizzata mediante collegamenti via cavo costituita da:

- N **1** server fisico dotato di dischi raid
- N **1** router
- N **6** postazioni di lavoro in area ufficio
- N **1** postazioni di lavoro in area produttiva
- N **6** stampanti/ fotocopiatrici MFP
- N **1** fax
- N **1** switch di rete

7.2.4 Elaboratori in rete pubblica (internet)

Sono collegati a internet i seguenti computer:

- N **6** postazioni di lavoro dislocate nell'area ufficio;
- N **1** postazioni dislocate nell'area produttiva.

Protezione del Sistema mediante:

- ESET ANTIVIRUS NOD32

Tipologia di software caricati sui PC:

Id Produttore	Nome Software	Versione
7ZIP	7ZIP	VARIA
BUSINESS OBJECTS	BUSINESS OBJECTS	4.1 SP5
QLICKTECH	QLICKVIEW	9.0.7320.7
NANOSYSTEMS SRL	SUPREMO RDP DESKTOP	VARIA
ADOBE	READER	VARIA
MICROSOFT	OFFICE	XP PRO / 2007 / 2013
MICROSOFT	SQL SERVER	2003
MICROSOFT	NAVISION	5.0 SP1
ZUCCHETTI	MAGO.NET	ND
ECOS	ECOS BASE	WEB

Backup eseguiti con frequenza:

- 1 volta al giorno per dati utenti, cartelle di rete e database gestionale, di notte su cartella locale server,

PC collegati mediante:

- Dominio in Area Uffici,

7.2.5 Piattaforme che utilizzano tecnologia web

- Nessuna

7.2.6 Mappa dei trattamenti effettuati

Dal riepilogo dei dati trattati, così come risulta anche nel registro dei trattamenti di cui all'art. 30 GDPR, che si allega al presente modello e dall'identificazione degli strumenti utilizzati si delinea il seguente schema:

Tipologia trattamento	*Cartaceo*	*Computer non in rete*	*Computer in rete privata*	*Computer in rete pubblica*	*Video sorveglianza*
Dati comuni relativi a clienti /fornitori	X		X		X
Dati comuni relativi a lavoratori	X		X		X
Dati relativi allo svolgimento di attività economiche/ commerciali	X		X		
Dati di natura giudiziaria dei lavoratori	X				
Dati idonei a rilevare lo stato di salute dei lavoratori	X		X		

7.2.7 Analisi dei trattamenti effettuati

Dalla rilevazione degli strumenti utilizzati e delle tipologie dei dati trattati emerge che:

- i dati personali vengono sistematicamente trattati con supporti cartacei e con elaborazione;
- i dati "particolari" trattati con elaborazione sono limitati a quelli necessari ad assolvere agli obblighi normativi e contrattuali con riferimento alla materia giuslavoristica; trattasi dei soli dati del personale dipendente;
- gli elaboratori in rete pubblica presenti dispongono esclusivamente del collegamento a internet.

7.3 Sede di Quinto di Treviso (TV)

7.3.1 Aree, locali e strumenti con i quali si effettuano i trattamenti

Gli uffici sono dislocati al piano terra. L'accesso all'immobile è controllato da portone d'ingresso con citofono e suoneria d'ingresso.
Le porte d'ingresso si presentano con chiavi di sicurezza.

7.3.2 Schedari e altri supporti cartacei

I supporti cartacei, contenenti dati sensibili sono raccolti in… custoditi in...

7.3.3 Elaboratori in rete privata

Il sistema di lavoro della struttura avviene con elaborazione in rete privata ethernet. Si dispone di una rete di lavoro realizzata mediante collegamenti via cavo costituita da:

- N **1** server fisico dotato di dischi raid
- N **1** router con access point wireless
- N **2** postazioni di lavoro in area ufficio
- N **1** stampante MFP
- N **1** switch di rete
- N **1** firewall hardware

7.3.4 Elaboratori in rete pubblica (internet)

Sono collegati a internet i seguenti computer:

- N **2** postazioni di lavoro dislocate nell'area ufficio;

Protezione del Sistema mediante:

- ESET ANTIVIRUS NOD32

Tipologia di software caricati sui PC:

Id Produttore	Nome Software	Versione
7ZIP	7ZIP	VARIA
NANOSYSTEMS SRL	SUPREMO RDP DESKTOP	VARIA
ADOBE	READER	VARIA
MICROSOFT	OFFICE	2007 / 2013
MICROSOFT	SQL SERVER	2003
MICROSOFT	NAVISION	5.0 SP1
ECOS	ECOS BASE	WEB

Backup eseguiti con frequenza:

- MAI – IL SERVER NON VIENE PIU' UTILIZZATO – SOLO PER DOMINIO E FIREWALL – GESTIONALE AD ISTRANA

PC collegati mediante:

- Dominio in Area Uffici,

7.3.5 Piattaforme che utilizzano tecnologia web

- Nessuna

7.3.6 Mappa dei trattamenti effettuati

Dal riepilogo dei dati trattati, così come risulta anche nel registro dei trattamenti di cui all'art. 30 GDPR, che si allega al presente modello e dall'identificazione degli strumenti utilizzati si delinea il seguente schema:

Tipologia trattamento	*Cartaceo*	*Computer non in rete*	*Computer in rete privata*	*Computer in rete pubblica*	*Video sorveglianza*
Dati comuni relativi a clienti /fornitori	**X**		**X**		
Dati comuni relativi a lavoratori	**X**		**X**		
Dati relativi allo svolgimento di attività economiche/ commerciali	**X**		**X**		
Dati di natura giudiziaria dei lavoratori	**X**				
Dati idonei a rilevare lo stato di salute dei lavoratori	**X**		**X**		

7.3.7 Analisi dei trattamenti effettuati

Dalla rilevazione degli strumenti utilizzati e delle tipologie dei dati trattati emerge che:

- i dati personali vengono sistematicamente trattati con supporti cartacei e con elaborazione;
- i dati "particolari" trattati con elaborazione sono limitati a quelli necessari ad assolvere agli obblighi normativi e contrattuali con riferimento alla materia giuslavoristica; trattasi dei soli dati del personale dipendente;
- gli elaboratori in rete pubblica presenti dispongono esclusivamente del collegamento a internet.

8 MISURE ATTE A GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI

(i contenuti del seguente paragrafo e dei sotto capitoli si riferiscono solo alla sede di Ospedaletto di Istrana, vanno integrati con quanto in essere presso le sedi secondarie)

Alla luce dei fattori di rischio e delle aree individuate nel presente paragrafo sono 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:

a. misure già adottate al momento della stesura del presente documento;
b. ulteriori misure finalizzate a incrementare il livello di sicurezza nel trattamento dei dati.

8.1 La protezione di aree e locali

Per quanto concerne il rischio che i dati vengano danneggiati o perduti a seguito di eventi distruttivi i locali ove si svolge il trattamento dei dati sono protetti da:

- gruppo di continuità dell'alimentazione elettrica;
- impianto di condizionamento.

Sono adottate le seguenti misure per impedire accessi non autorizzati:

- dotazione di cancello elettrico;
- telecamera per controllo ingressi.

8.2 Custodia e archiviazione dei dati

Ai soggetti "autorizzati al trattamento" dei dati particolari sono state impartite istruzione per la gestione, la custodia e l'archiviazione dei documenti e dei supporti. In particolare sono state fornite direttive per:

- il corretto accesso ai dati personali, sensibili e giudiziari;
- la conservazione e la custodia di documenti, atti e supporti contenenti dati personali, sensibili e giuridici;
- la definizione delle persone autorizzate ad accedere ai locali archivio e le modalità di accesso.

8.3 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 "autorizzati al trattamento" possono accedere o utilizzare al fine delle proprie mansioni lavorative;
- protezione di strumenti e dati da malfunzionamento e attacchi informatici;

8.4 Accesso ai dati e istruzioni impartite agli incaricati

Gli incaricati al trattamento dei dati dovranno osservare le seguenti istruzioni per l'utilizzo degli strumenti informatici nonché attenersi al regolamento aziendale sull'utilizzo degli strumenti informatici:

- obbligo di custodire i dispositivi di accesso agli strumenti informatici (password);
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento;
- obbligo di assoluta riservatezza;
- divieto di divulgazione della password di accesso al sistema.

8.5 Protezione di strumenti e dati

Il sistema di elaborazione è, comunque, protetto da programmi antivirus e di sistema firewall antintrusione.
Il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione.
Il backup dei dati viene effettuato con cadenza giornaliera.
Agli "autorizzati al trattamento" è stato affidato il compito di aggiornare le password ogni sei mesi.

8.6 Supporti rimovibili

Anche se le norme prevedono particolari cautele solo per i supporti rimovibili contenenti dati sensibili ("dati particolari") e giuridici, la tutela per il trattamento viene estesa ai dati personali come segue:

- cancellazione e/o distruzione dei summenzionati supporti, una volta cessate le ragioni per la conservazione.

9 CRITERI E MODALITÀ DI RIPRISTINO DEI DATI

Per i dati trattati con strumenti elettronici sono previste procedure di backup attraverso le quali è periodicamente effettuata una copia di tutti i dati presenti nel sistema.
Il salvataggio dati avviene:

- con frequenza giornaliera;
- le copie vengono custodite in un luogo protetto (cassaforte ignifuga).

10 AFFIDAMENTO DEI DATI PERSONALI ALL'ESTERNO

Nello svolgimento dell'attività di norma non vengono affidati dati personali all'esterno.
Nel caso il trattamento venga affidato all'esterno saranno impartite istruzioni per iscritto al terzo destinatario, al fine di rispettare quanto prescritto dal codice della privacy.

11 CONTROLLO GENERALE SULLO STATO DI SICUREZZA

Il Titolare del Trattamento Dati (l'Azienda) cui compete le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, mantiene aggiornate le misure di sicurezza al fine di adottare gli strumenti più idonei per la tutela dei dati trattati.
Il Titolare del Trattamento Dati verifica con frequenza almeno mensile l'efficacia delle misure adottate relativamente a:

- accesso fisico ai locali dove si svolge il trattamento;
- procedure di archiviazione e custodia dei dati trattati;
- efficacia e utilizzo delle misure di sicurezza degli strumenti elettronici;
- integrità dei dati e delle loro copie di backup;
- distruzione dei supporti non più riutilizzabili;
- livello di informazione degli interessati.

12 VIOLAZIONE E/O PERDITA DEL DATO PERSONALE (DATA BREACH)

Le principali responsabilità ed attività relative agli obblighi di notifica verso organismi di controllo degli incidenti di sicurezza delle informazioni che abbiano come conseguenza la violazione di dati personali (*data breach*) sono regolati dalla procedura di gruppo P164 "notifica degli incidenti di sicurezza delle informazioni" alla quale si rimanda.

13 ORGANIGRAMMA AZIENDALE DELLA PRIVACY

TITOLARI DEL TRATTAMENTO

ALIPLAST S.P.A., VIA FORNACI 14 Cap 31036 – ISTRANA (TV) Codice Fiscale 00792100265 Partita IVA 00792100265 - Codice ATECO 22.21.00 (riconducibile alla figura dell'amministratore delegato della società)

RAPPRESENTANTE DEL TITOLARE DEL TRATTAMENTO

Il titolare del trattamento ha deciso di nominare quale suo rappresentante il Sig. Rupolo Roberto.

RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI DELL'UNITA' ORGANIZZATIVA

I Direttori ed i responsabili di funzione (vedasi l'organigramma aziendale) rappresentano la struttura organizzativa di supporto al titolare (RUO di 1° livello il rappresentante, RUO di 2° livello le altre figure di responsabili) nello svolgimento dei compiti e delle attività legati al loro ambito di competenza e relativi al trattamento di dati personali.

RESPONSABILI ESTERNI DEL TRATTAMENTO

Con riferimento all'assistenza e consulenza fiscale, Studio Lot Manzan ed associati, Piazza Aldo Moro, 6, 31020 Lancenigo.
I rapporti con i suddetti soggetti sono regolarmente disciplinati con apposti documenti contrattuali.

AMMINISTRATORE DI SISTEMA

Il Responsabile del Trattamento ha nominato come Amministratore di Sistema Informatico il Dott. Casarin Fabio e Sig. Bordin Emanuele.

PERSONALE AUTORIZZATO AL TRATTAMENTO

Al momento, sono stati nominati per iscritto i diversi soggetti "autorizzati al trattamento", a ciascuno dei quali è stata consegnata una specifica lettera di incarico individuale, nella quale sono fornite precise istruzioni sulle modalità di effettuazione del trattamento e sulle misure di sicurezza da osservare.
Si è provveduto a nominare per iscritto "l'amministratore del sistema informativo": il sig. [*NOME E COGNOME*], al fine di garantire una migliore efficienza e tutela del sistema informativo.

Il presente modello di organizzazione e gestione della privacy è soggetto a monitoraggio continuo da parte del titolare dovendo essere aggiornato ogniqualvolta si renda necessario in ragioni di mutamenti nel modo di operare della ditta o di novità legislative.
Il presente documento è aggiornato al 03.08.2018

Istrana, lì 07.01.2019