ISTITUTO ZOOPROFILATTICO SPERIMENTALE DEL LAZIO E DELLA TOSCANA M. ALEANDRI

DELIBERAZIONE DEL DIRETTORE GENERALE

n. 623 del 22/11/2018

OGGETTO: Adempimenti in materia di "Privacy" ai sensi del Regolamento UE 2016/679: approvazione del *Documento relativo al trattamento dei dati personali.*

Proposta di deliberazione n. **del**

Direzione Generale

L'Estensore Daniele D'Alberto

Il Responsabile del procedimento [illegible]

Visto di regolarità contabile ..... **n° di prenot.** .....

Parere del Direttore Amministrativo ☒ Favorevole ☐ Non favorevole
F.to Avv. Mauro Pirazzoli .....

Parere del Direttore Sanitario ☒ Favorevole ☐ Non favorevole
F.to Dott. Andrea Leto.....

IL DIRETTORE GENERALE
F.to Dott. Ugo Della Marta

IL DIRETTORE GENERALE

OGGETTO: Adempimenti in materia di "Privacy" ai sensi del Regolamento UE 2016/679: approvazione del *Documento relativo al trattamento dei dati personali*

Visto:

- Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018;
- Il D.Lgs. n. 101 del 10 agosto 2018 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*", che ha modificato il codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;

Considerato che:

- L'Istituto con Delibera n° 272 del 21/05/2018 ha designato il Responsabile della Protezione dei Dati personali (RDP) ai sensi dell'art. 37 del Regolamento UE 2016/679;

- L'art. 30 del Regolamento (UE) n. 679/2016 prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del "Registro delle attività di trattamento";

- Risulta necessario formalizzare il ***Documento relativo al trattamento dei dati personali***, allegato alla presente delibera di cui forma parte integrante, che contiene al suo interno anche il "Registro delle attività di trattamento";
- Il ***Documento relativo al trattamento dei dati personali*** indica le strutture interne ed esterne all'Istituto che trattano i dati ai sensi del Regolamento UE 2016/679;

- Nell'attesa della completa applicazione del Regolamento per l'ordinamento interno dei Servizi dell'Istituto adottato con Delibera del Consiglio di Amministrazione n. 8 del 22 novembre 2017, attraverso l'attribuzione dei relativi incarichi, risulta altresì necessario individuare i Responsabili Interni del trattamento dei dati;
- Risulta inoltre opportuno procedere alla nomina dei Responsabili Esterni del trattamento dei dati, ai sensi di quanto previsto nel paragrafo "Affidamento di trattamenti di dati personali all'esterno" del ***Documento relativo al trattamento dei dati personali,*** richiedendo ai medesimi di indicare nominativamente i loro incaricati del trattamento dei dati dell'Istituto in loro possesso;

Visti i pareri conformi del Direttore Sanitario e Amministrativo;

DELIBERA

1. di approvare il "Documento relativo al trattamento dei dati personali", allegato 1, parte integrante del presente provvedimento, che contiene al suo interno il *Registro delle attività di trattamento*, ai sensi dell'Art. 30 del Regolamento UE n. 679/2016.
2. Di individuare quali Responsabili Interni del trattamento dei dati i Responsabili delle strutture indicate nel *Registro delle attività di trattamento*, ai sensi dell'art. 28 comma 3 del Regolamento UE 2016/679 come da elenco allegato 2, parte integrante del presente provvedimento;
3. Di procedere alla nomina dei Responsabili Esterni del trattamento dati, individuati nei rappresentanti legali delle strutture esterne presenti nel *Registro delle attività di trattamento* di cui al punto 1 della presente deliberazione, ai sensi dell'art. 28 comma 3 del Regolamento UE 2016/679. come da elenco allegato 3, parte integrante del presente provvedimento.

IL DIRETTORE GENERALE
F.to Dott. Ugo Della Marta

PUBBLICAZIONE

Copia della presente deliberazione è stata pubblicata ai sensi della legge 69/2009 e successive modificazioni ed integrazioni in data 22/11/2018.

IL FUNZIONARIO INCARICATO
F.to Sig.ra Eleonora Quagliarella

ALLEGATO 1

Istituto Zooprofilattico Sperimentale
del Lazio e della Toscana *M. Aleandri*

Documento relativo al trattamento dei dati personali

Oggetto

Il presente documento descrive le misure organizzative, fisiche e logiche che il titolare del trattamento dei dati deve adottare affinché siano rispettati gli obblighi previsti dal Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e dal D.Lgs. n. 196/2003, codice in materia di protezione dei dati personali, come modificato dal D.Lgs. 10 agosto 2018, n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati*". Tali misure sono definite con lo scopo di evitare trattamenti non autorizzati o illeciti, la perdita, la distruzione o il danno accidentale.

Titolare del trattamento dei dati

Istituto Zooprofilattico Sperimentale del Lazio e della Toscana '*M. Aleandri*' (Istituto), Roma - Via Appia Nuova, 1411, - 00178 – Tel. 06 790991 - Fax 06 79340724 – www.izslt.it – info@izslt.it, pec izslt@legalmail.it.

Responsabile della protezione dei dati

Dr. Renato Colafrancesco, Istituto Zooprofilattico Sperimentale del Lazio e della Toscana 'M. Aleandri', Data Protection Office, Roma - Via Appia Nuova, 1411, - 00178 – Tel. 06 79099325 - Fax 06 79099462 - privacy@izslt.it.

Ambito di applicazione

Si applica al trattamento di dati personali interamente o parzialmente automatizzato o non automatizzato, contenuti in un archivio informatizzato o cartaceo o destinati a figurarvi.

Principi applicabili al trattamento di dati personali

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato e raccolti per finalità determinate, esplicite e legittime. Non devono essere trattati per finalità diverse da quelle per cui sono stati raccolti. Possono essere trattati a fini di archiviazione nel pubblico interesse, di ricerca scientifica, a fini statistici.

I dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario, esatti, aggiornati e conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati trattati.

Deve essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative proporzionate.

Finalità della raccolta dei dati personali e base giuridica del trattamento (liceità)

Il trattamento è lecito se l'interessato ha espresso il consenso oppure è necessario per: eseguire un contratto, adempiere ad un obbligo legale, la salvaguardia degli interessi vitali dell'interessato, l'esecuzione di un compito di interesse pubblico, il perseguimento del legittimo interesse dal titolare.

L'Istituto tratta i dati personali di persone fisiche, persone giuridiche, ditte individuali e liberi professionisti per:

	Finalità	Base giuridica che legittima il trattamento	Consenso	Obbligatorietà del dato
01	Istituzionali (norme sull'ordinamento degli IIZZSS)	SI	NO	SI
02	necessità di eseguire un contratto di cui l'Interessato sia parte o di eseguire attività precontrattuali su sua richiesta	SI	NO	SI
03	necessità di adempiere ad obblighi legali (es. obblighi previsti dalla normativa antiriciclaggio, disposizioni impartite da Autorità di Vigilanza, dalla Magistratura, ecc.).	SI	NO	SI
04	comunicazione, promozione e vendita di prodotti e servizi dell'Istituto, compreso il compimento di ricerche di mercato	NO	SI	NO
05	comunicazione, promozione e vendita di prodotti e servizi specificatamente individuati attraverso l'elaborazione e l'analisi, anche mediante l'impiego di tecniche o sistemi automatizzati (es. big data), di informazioni relative a preferenze, abitudini, scelte di consumo, finalizzate a suddividere gli interessati in gruppi omogenei per comportamenti o caratteristiche specifiche (profilazione della clientela) attuate anche attraverso l'arricchimento dei dati con informazioni acquisite da soggetti terzi	NO	SI	NO

Condizioni per il consenso

Qualora il trattamento sia basato sul consenso, il titolare deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. Se il consenso è presentato in forma scritta, la richiesta deve essere comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

Categorie di dati trattati

L'Istituto tratta dati personali raccolti direttamente presso l'interessato, ovvero presso terzi, che includono, a titolo esemplificativo, dati anagrafici (es. nome, cognome,indirizzo,data e luogo di nascita, codice fiscale e/o partita IVA, indirizzo di posta elettronica), informazioni sulla situazione finanziaria

(es. situazione patrimoniale, informazioni creditizie che attengono a richieste/rapporti di fornitura), dati relativi all'immagine (es. foto su carta d'identità) e altri dati riconducibili alle categorie sopra indicate.
L'Istituto non richiede e non tratta di sua iniziativa dati particolari sensibili della propria clientela (es. dati che rivelino l'origine razziale o etnica, le opinioni politiche, e le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, biometrici - intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona). Tuttavia è possibile che, per dare esecuzione a specifiche richieste di servizi e operazioni inerenti il rapporto con i propri dipendenti o fornitori (es. il pagamento di quote associative a partiti o sindacati, bonifici ad associazioni, situazioni patrimoniali o creditizie ecc.) l'Istituto debba trattare tali dati. Per il personale dipendente, possono altresì essere trattati dati inerenti lo stato di salute suo o di suoi familiari (es. stato di invalidità permanente o temporaneo o malattie inabilitanti).
Poiché l'Istituto non può intercettare o rifiutare queste richieste, la proposta di contratto non potrà essere accettata qualora l'interessato non abbia dichiarato il proprio consenso scritto al suddetto trattamento. I dati in questione verranno trattati esclusivamente per dare esecuzione alla richiesta dell'interessato.

Diritti dell'interessato

Il titolare adotta misure appropriate per fornire all'interessato tutte le informazioni previste in forma concisa, trasparente, intellegibile e facilmente accessibile, con linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto, con mezzi elettronici, oralmente se richiesto dall'interessato, purché sia comprovata con altri mezzi l'identità dell'interessato.
Il titolare fornisce all'interessato, nel momento in cui i dati sono raccolti: l'identità ed i dati di contatto del titolare, del responsabile della protezione dei dati, le finalità per cui i dati sono raccolti e la base giuridica del trattamento, gli eventuali destinatari dei dati, l'intenzione di trasferire i dati ad un paese terzo, il periodo di conservazione, l'esistenza del diritto dell'interessato di chiedere l'accesso ai dati personali, la rettifica, la cancellazione o la limitazione del trattamento o di opporsi allo stesso, oltre al diritto di portabilità dei dati. Inoltre l'interessato ha il diritto di revocare il consenso e di proporre reclamo ad un'autorità di controllo.

Sicurezza dei dati personali

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio: pseudonimizzazione e cifratura dei dati; capacità di assicurare la riservatezza, l'integrità, la disponibilità, la resilienza dei sistemi e di servizi di trattamento; capacità di ripristinare la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico; testare, verificare e valutare l'efficacia delle misure tecniche e organizzative; valutare il livello di sicurezza in funzione del rischio di distruzione, perdita, modifica, divulgazione non autorizzata, accesso accidentale o illegale ai dati; chiunque abbia accesso a dati personali deve essere istruito al trattamento di tali dati.

Notifica di violazione

In caso di violazione di dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che la violazione non presenti un rischio per i diritti e le libertà delle persone fisiche.

Quando la violazione presenta un rischio per le persone fisiche, il titolare comunica la violazione all'interessato senza ingiustificato ritardo.

Registro delle attività di trattamento (Ex art. 30 del Regolamento UE n. 679/2016)

Registro delle attività di trattamento										
Titolare del trattamento: Dr. Ugo Della Marta Direttore Generale					Istituto Zooprofilattico Sperimentale del Lazio e della Toscana 'M. Aleandri', Roma - Via Appia Nuova, 1411, - 00178 – Tel. 06 790991 - Fax 06 79340724 – www.izslt.it – info@izslt.it, pec izslt@legalmail.it.					
Responsabile per la protezione dei dati: Dr. Renato Colafrancesco					Istituto Zooprofilattico Sperimentale del Lazio e della Toscana 'M. Aleandri', Data Protection Office, Roma - Via Appia Nuova, 1411, - 00178 – Tel. 06 79099325 - Fax 06 79099462 - privacy@izslt.it.					
Nr.	Strutture	natura dei dati			Finalità	Trattamento	Categorie interessate	Tipi di dati	strutture esterne che concorrono	Denominazione archivio o banca dati
		personali	sensibili	giudiziari						
01	Ufficio di supporto alla direzione aziendale				Videosorveglianza	immagini	dipendenti, visitatori	video	Sicurezza	
02	U.S. Formazione	X			corsi di formazione ECM	anagrafica per la partecipazione ai corsi	Dipendenti, Clienti	anagrafici	Ministero Salute	Portale formazione, Archivio cartaceo corsi ECM
03	U.S. Formazione	X			corsi di formazione no ECM	anagrafica per la partecipazione ai corsi	Dipendenti, Clienti	anagrafici		Portale formazione, Archivio cartaceo corsi no ECM
04	U.S. Formazione	X			sito web - News	anagrafica persone iscritte alle news	Clienti	anagrafici		sito web IZS - News
05	U.S. Osservatorio Epidemiologico	X			analisi statistiche, sorveglianza epidemiologica, debiti informativi					

06	U.S. Osservatorio Epidemiologico	X			Prestazioni sanitarie	Anagrafiche clienti	Clienti	anagrafici	New genesys	SIL
07	U.S. Sistemi informatici	X			servizi all'utenza esterna	Anagrafica utenti	Utenti, Cliente, Libero professionista, dipendenti enti SSN	anagrafici		SIEV
08	U.S. Sistemi informatici	X			Prestazioni sanitarie	Anagrafiche clienti	Clienti	anagrafici	New genesys	SIL
09	U.S. Sistemi informatici	X			sito web - News	anagrafica persone iscritte alle news	Clienti	anagrafici		sito web IZS - News
10	U.S. Sistemi informatici	X			sito web - Convenzioni	Anagrafiche clienti	Clienti	anagrafici		sito web IZS - Convenzioni
11	U.S. Sistemi informatici	X			corsi di formazione ECM	anagrafica per la partecipazione ai corsi	Dipendenti, Clienti	anagrafici	Ministero Salute	Portale formazione
12	U.S. Sistemi informatici	X			corsi di formazione no ECM	anagrafica per la partecipazione ai corsi	Dipendenti, Clienti	anagrafici		Portale formazione
13	U.S. Sicurezza e prevenzione sui luoghi di lavoro	X	X		Sorveglianza medica di cui alla normativa di tutela dei lavoratori	anagrafe dipendenti, stato di salute	Dipendenti	anagrafici, stato di salute	Medico del lavoro	Archivio cartaceo catelle cliniche
14	U.S. Qualità	X			accreditamento procedure	anagrafe dipendenti, curriculum	Dipendenti	anagrafici		Archivio curriculum qualità
15	U.S. Ricerca ed innovazione	X			ricerca e progetti	anagrafe partner, curriculum	Partner	anagrafici	Oslo	Rcubo, Archivio ricerche e progetti
16	D.O. Risorse umane e affari legali	X	X	X	Trattamento economico, giuridico e previdenziale, malattie, sindacali, maternità, prestiti, trattenute coatte	Anagrafica dipendenti, famiglia, istruzione, lavoro, presenze orarie	Dipendente	anagrafici, economici, salute, giudiziari, categorie protette, presenze	INAZ paghe	INAZ, Archivio cartaceo del personale, fascicilo del dipendente
17	D.O. Risorse umane e affari legali	X	X	X	selezione e assunzione del personale	Anagrafica concorrenti, curriculum	Partecipanti concorsi	anagrafici, categorie protette, casellario giudiziario		Archivio cartaceo curriculum concorsi
18	D.O. Acquisizione beni e servizi	X	X	X	Acquisto beni e servizi, espletamento gare	Anagrafica fornitori	Fornitore	anagrafici, patrimonio, documenti identità, condanne	ESG Services, Eldasoft, Althea group	AS400, Portale Appalti, Sigeco, Archivio cartaceo Fornitori e gare
19	D.O. Economico finanziaria e controllo di gestione	X			Pagamento fatture	Anagrafica fornitori	Fornitore	anagrafici	ESG Services	AS400
20	D.O. Economico finanziaria e controllo di	X			Pagamento prestazioni professionali	Anagrafica consulenti	Liberi professionisti	anagrafici	ESG Services	AS400

	gestione									
21	D.O. Economico finanziaria e controllo di gestione	X	X		Controllo di gestione	Anagrafica dipendenti	Dipendente	anagrafici, economici	Oslo	Rcubo
22	D.O. Economico finanziaria e controllo di gestione	X			fatturazione prestazioni sanitarie	Anagrafica clienti	Cliente	anagrafici	ESG Services	AS400
23	D.O. Tecnico patrimoniale e ingegneria clinica	X			Collaudi, Manutenzioni	Anagrafica fornitori	Fornitore	anagrafici	Althea group	EASI, Sigeco, Archivio cartaceo fornitori
24	D.O e U.S. tutte	X			controllo delle presenze	presenze orarie	Dipendente	presenze	INAZ paghe	INAZ
25	D.O. Accettazione e servizi interdisciplinari, D.O.Territoriali	X			fatturazione prestazioni sanitarie	Anagrafica clienti	Cliente	anagrafici	ESG Services	AS400
26	D.O. Accettazione e servizi interdisciplinari, D.O.Territoriali	X			prestazioni sanitarie	Anagrafica clienti	Cliente	anagrafici	New genesys	SIL, Archivio cartaceo richieste
27	D.O. Accettazione e servizi interdisciplinari, D.O.Territoriali	X			prestazioni sanitarie	Anagrafica clienti	Cliente	anagrafici	Enti SSN, Regione Lazio	SIEV
28	D.O. Sanitarie tutte	X			prestazioni sanitarie	Anagrafica clienti	Cliente	anagrafici	New Genesis	SIL, Archivio cartaceo rapporti prova
29	D.O. Sanitarie tutte	X			ricerca e progetti	anagrafe partner, curriculum	Partner	anagrafici	Oslo	Rcubo, Archivio ricerche e progetti
30	D.O. e U.S. tutte	X			accreditamento procedure	anagrafe dipendenti, curriculum	Dipendenti	anagrafici		Archivio curriculum qualità

Banche dati e archivi presenti

Banche dati					
	Denominazione archivio o banca dati	**Tipo archivio**	**Ubicazione**	**dispositivi di accesso**	**soggetti esterni abilitati**
01	Portale formazione	informatico	sala server	credenziali	
02	Archivio cartaceo corsi ECM	cartaceo	U.S. Formazione	fisico autorizzato	
03	Archivio cartaceo corsi no ECM	cartaceo	U.S. Formazione	fisico autorizzato	
04	sito web IZS - News	informatico	sala server	credenziali	
05	sito web IZS - Convenzioni	informatico	sala server	credenziali	
06	SIL	informatico	sala server	credenziali	New genesys
07	SIEV	informatico	sala server	credenziali	

08	Archivio cartaceo catelle cliniche	cartaceo	Ufficio medico	fisico autorizzato	Medico
09	Archivio curriculum qualità	informatico	Personal computer distribuito D.O. e U.S.	credenziali	
10	Rcubo	informatico	sala server	credenziali	Oslo
11	Archivio ricerche e progetti	informatico	Personal computer distribuito D.O. sanitarie	credenziali	
12	INAZ	informatico	sala server	credenziali	INAZ paghe
13	Archivio cartaceo del personale, fascicilo del dipendente	cartaceo	D.O. Risorse umane e affari generali	fisico autorizzato	
14	Archivio cartaceo curriculum concorsi	cartaceo	D.O. Risorse umane e affari generali	fisico autorizzato	
15	Archivio cartaceo Fornitori e gare	cartaceo	D.O. Acquisizione beni e servizi	fisico autorizzato	
16	Sigeco	informatico	D.O. Tecnico patrimoniale e ingegneria clinica	credenziali	Althea group
17	EASI	informatico	D.O. Tecnico patrimoniale e ingegneria clinica	credenziali	Althea group
18	AS400	informatico	sala server	credenziali	ESG Services
19	Portale Appalti	informatico	sala server	credenziali	Eldasoft
20	Archivio cartaceo richieste	cartaceo	distribuito D.O. sanitarie	fisico autorizzato	
21	Archivio cartaceo rapporti prova	cartaceo	distribuito D.O. sanitarie	fisico autorizzato	

Archivi cartacei

Gli archivi sono conservati in luoghi protetti e/o armadi muniti di serratura con accesso consentito esclusivamente al titolare o agli incaricati dei trattamenti. L'accesso agli archivi cartacei che contengono dati sensibili o giudiziari è di tipo controllato e selezionato con l'individuazione degli incaricati autorizzati a visionare gli archivi stessi.

L'accesso ai documenti può avvenire esclusivamente durante l'orario lavorativo. Le persone a cui è consentito l'accesso ai dati sensibili o giudiziari, al di fuori dell'orario lavorativo, sono identificate e registrate.

Il trasferimento di documenti da cui si può risalire a dati personali e/o sensibili viene attuato utilizzando custodie protettive la cui chiusura ed apertura viene consentita esclusivamente al titolare o agli incaricati del trattamento. Non è consentito lasciare incustoditi documenti che riportano dati personali.

Archivi informatici

Il sistema informativo dell'Istituto è composto da 9 sottosistemi dislocati presso la sede centrale e le sedi territoriali collegati con connessioni in fibra ottica e HDSL. E' stata realizzata una VPN (Virtual Private Network) protetta da dispositivi Firewall, utilizzando internet come tecnologia di trasporto. Nella rete privata dell'Istituto, LAN, è stata creata una sottorete, DMZ, destinata a contenere i sistemi che devono essere isolati dalla rete interna e destinata a contenere i servizi raggiungibili dall'esterno. Alla rete interna sono collegate circa 500 stazioni di lavoro ubicate nelle aree di lavoro.

Le credenziali di autenticazione per l'accesso alla rete ed ai sistemi sono il codice identificativo dell'incaricato, associato ad una parola chiave. Ad ogni incaricato possono essere associati più codici identificativi e parole chiave in funzione delle banche dati a cui accede. Dove è consentito, le parole chiave hanno una lunghezza almeno di otto caratteri e sono modificate dall'incaricato al loro primo utilizzo e, successivamente, ogni sei mesi. In caso di trattamenti di dati sensibili e di dati giudiziari, la parola chiave è modificata almeno ogni tre mesi. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per scopi di gestione tecnica. I dati contenuti in archivi informatizzati vengono salvati mediante copie di sicurezza giornaliere, settimanali e mensili al fine di prevenire la perdita definitiva di dati in caso di eventi malevoli accidentali o intenzionali.

Sistemi accessibili dalla rete pubblica

Tutti i sistemi accessibili dalla rete pubblica (internet) sono collocati in area DMZ e protetti da firewall.

Videosorveglianza

Il sistema di videosorveglianza è composto complessivamente da 12 videocamere dislocate all'interno dell'Istituto di cui 4 all'interno dei fabbricati e 8 all'esterno.

Le immagini vengono registrate su supporti magnetici, secondo cicli giornalieri di riutilizzo dei supporti stessi. I supporti sono conservati in appositi armadi protetti da chiave il cui accesso è consentito ai soli titolari, responsabili e incaricati dei trattamenti.

Distribuzione dei compiti e delle responsabilità degli incaricati

Sono individuati i seguenti livelli di responsabilità relativi al trattamento dei dati:

- **Titolare del trattamento**

Il titolare del trattamento dei dati è l'Istituto, legalmente rappresentato dal Direttore Generale e determina le finalità ed i mezzi del trattamento di dati personali. Mette in atto misure tecniche ed organizzative adeguate per garantire e dimostrare che il trattamento è effettuato conformemente al regolamento (UE) 2016/679, incluso l'attuazione di politiche idonee.

Il titolare del trattamento affida il trattamento di alcune categorie di dati all'esterno dell'amministrazione: i gestori dei dati esterni devono assicurare che tali dati siano gestiti in conformità al regolamento sopra citato. I soggetti esterni devono essere nominati a tutti gli effetti responsabili del trattamento, con i quali stipulare regolare contratto.

L'operatività e la sicurezza del sistema, in caso di prolungata assenza o impedimento del titolare, sono garantite dal Direttore Sanitario o, in sua assenza, dal Direttore Amministrativo.

- **Responsabile del trattamento**

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, questo ricorre a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento (UE) 2016/679 e garantisca la tutela dei diritti dell'interessato. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico.

Qualora il titolare ritenga di non nominare il responsabile del trattamento, ne assume tutte le responsabilità e funzioni.

Il responsabile del trattamento dei dati personali ha il compito di:

- nominare e redigere la lista degli incaricati del trattamento dei dati personali, limitatamente alle banche dati di cui è responsabile;
- aggiornare annualmente la lista degli incaricati;
- mettere a disposizione di ciascun incaricato le norme che riguardano la sicurezza ed il trattamento dei dati in vigore;
- sorvegliare che il trattamento sia effettuato in osservanza delle disposizioni del regolamento sopra citato e del presente documento;

- dare le adeguate istruzioni agli incaricati del trattamento dei dati che devono riportare almeno i seguenti requisiti minimi:
  - dovere di custodire i dispositivi e gli strumenti, attribuiti agli incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere ai sistemi informativi e archivi cartacei;
  - obbligo di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
  - dovere di elaborare in modo appropriato la password e di conservare la segretezza della stessa, nonché delle altre componenti riservate delle credenziali di autenticazione, attribuite dall'amministratore di sistema;
  - di accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
  - verificare periodicamente, e comunque annualmente, la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati del trattamento dei dati personali, segnalando le modifiche agli incaricati della custodia delle copie delle credenziali.

Il responsabile del trattamento dei dati deve avere particolare attenzione alla gestione dei dati personali affidata a soggetti esterni attraverso la definizione di istruzioni scritte sulle modalità di trattamento e conservazione dei dati.

- **Responsabile della protezione dei dati**

Il titolare del trattamento, con delibera del Direttore Generale n. 272 del 21/05/2018 ha designato il Dr. Renato Colafrancesco come responsabile della protezione dei dati personali (RPD). E' incaricato almeno di informare e fornire consulenza in merito agli obblighi derivanti dal regolamento (UE) 2016/679, sorvegliarne l'osservanza nonché le politiche adottate in materia di protezione dei dati personali compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo, fornire un parere in merito alla valutazione di impatto sulla protezione dei dati.

- Incaricati del trattamento dei dati

Gli incaricati sono identificati con tutto il personale nonché con tutti i soggetti che hanno rapporti di collaborazione con l'Istituto che trattino dati personali in funzione delle mansioni attribuite nell'ambito della struttura di assegnazione.

Gli incaricati del trattamento dei dati personali devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli incaricati del trattamento dei dati personali deve essere assegnata una credenziale di autenticazione e copia delle chiavi fisiche degli archivi cartacei.

Per il trattamento dei dati personali gli incaricati osservano le seguenti disposizioni:

- effettuano esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto dell'incarico, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali;
- effettuano esclusivamente trattamenti di dati in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati;
- prestano particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, provvedono ad aggiornarli tempestivamente;
- osservano tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione o perdita anche accidentale dei dati, accessi non autorizzati, trattamenti non consentiti, o non conformi alle finalità della raccolta;
- conservano con la massima segretezza le componenti riservate delle credenziali di autenticazione ed i dispositivi di autenticazione in loro possesso;
- al termine dell'orario di lavoro riportano tutti i documenti cartacei nei locali individuati per la loro conservazione.

La tabella seguente definisce la struttura delle responsabilità all'interno dell'istituto ed i trattamenti dati che sono autorizzati ad effettuare:

Strutture	trattamenti operati dalla struttura
Ufficio di supporto alla direzione aziendale	01 - 24 - 30
U.S. Formazione	02 - 03 - 04 - 24 - 30

U.S. Osservatorio Epidemiologico	05 - 06 - 24 - 30
U.S. Sistemi informatici	07 - 08 - 09 - 10 - 11 - 12 - 24 - 30
U.S. Sicurezza e prevenzione sui luoghi di lavoro	13 - 24 - 30
U.S. Qualità	14 - 24 - 30
U.S. Ricerca ed innovazione	15 - 24 - 30
D.O. Risorse umane e affari legali	16 - 17 - 24 - 30
D.O. Acquisizione beni e servizi	18 - 24 - 30
D.O. Economico finanziaria e controllo di gestione	19 - 20 - 21 - 22 - 24 - 30
D.O. Tecnico patrimoniale e ingegneria clinica	23 - 24 - 30
D.O. Microbiologia degli alimenti	24 - 28 - 29 - 30
D.O. Chimica	24 - 28 - 29 - 30
D.O. Terreni e progetti speciali	24 - 29 - 30
D.O. Ricerca e controllo degli organismi geneticamente modificati	24 - 28 - 29 - 30
D.O. Diagnostica generale	24 - 28 - 29 - 30
D.O. Virologia	24 - 28 - 29 - 30
D.O. Sierologia	24 - 28 - 29 - 30
D.O. Accettazione e servizi interdisciplinari	24 - 25 - 26 - 27 - 28 - 29 - 30
D.O. Igiene delle produzioni e salute animale	24 - 28 - 29 - 30
D.O. Toscana nord	24 - 25 - 26 - 27 - 28 - 29 - 30
D.O. Toscana Centro	24 - 25 - 26 - 27 - 28 - 29 - 30
D.O. Toscana sud	24 - 25 - 26 - 27 - 28 - 29 - 30
D.O. Lazio nord	24 - 25 - 26 - 27 - 28 - 29 - 30
D.O. Lazio sud	24 - 25 - 26 - 27 - 28 - 29 - 30

Formazione degli incaricati al trattamento

Agli incaricati del trattamento, il responsabile fornisce 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.

Sarà inoltre fornito agli incaricati la procedura per l'uso delle risorse informatiche che rappresenta un valido ausilio informativo per supportare gli stessi nell'applicazione delle misure di sicurezza.

La formazione riguarderà:

- le norme generali in materia di privacy;
- gli aspetti peculiari dei trattamenti effettuati;
- gli aspetti legati alla progettazione ed implementazione delle misure di sicurezza.

Analisi dei rischi cui sono soggetti i dati personali ed individuazione delle misure di prevenzione

L'analisi dei possibili rischi che gravano sui dati è stata effettuata rispetto ai seguenti criteri:

- analisi degli eventi che possono generare rischi di distruzione, d'integrità e riservatezza dei dati;
- analisi dei rischi legati al trattamento dei dati rispetto ai diversi strumenti usati;
- individuazione delle misure per la minimizzazione e prevenzione dei rischi individuati.

Analisi del rischio sicurezza dei dati personali

Evento rischio	Impatto sulla sicurezza dei dati		Misure di azione
	descrizione	gravità	
Furto di credenziali di autenticazione	possibilità di furto delle credenziali di autenticazione	medio basso	gli accessi dall'esterno tramite rete internet sono protetti da firewall o autorizzati ad amministratori di sitema;
			regole di modifica periodica delle password;
			monitoraggio dell'utilizzo delle utenze;
			istruzione agli incaricati per la custodia in luogo sicuro delle credenziali;
			sorveglianza nei luoghi di lavoro da parte dei responsabili;
			conservazione delle credenziali in armadio o scrivania con serratura, in locale con porta chiusa;
			regole agli incaricati per la definizione sicura di password (complessità della password);
			divieto per gli utilizzatori di strumenti elettronici e informatici di lasciare incustodito o accessibile lo strumento stesso;
			utilizzo di portatili con politica di non memorizzare dati personali, sensibili e giudiziari.
Carenza di consapevolezza, disattenzione, incuria (eventi relativi ai comportamenti degli operatori)	possibile accesso di persone non autorizzate agli strumenti per il trattamento di dati cartacei o elettronici	medio basso	gestione della profilazione degli utenti;
			divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro;
			attivazione di azioni di formazione agli incaricati sulle tematiche di sicurezza dati;
			realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici;
			gli accessi dall'esterno tramite rete internet sono protetti da firewall o autorizzati ad amministratori di sitema;
			prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali;
			ogni incaricato è dotato di password e username univoci e personali costituenti le sue credenziali d'autenticazione;
			i codici identificativi personali sono disattivati in caso di non utilizzo per più di sei mesi;
			l'Istituto adotta le procedure di backup con cadenza giornaliera, settimenale e mensile per i dati contenuti sui server;
			l'accesso ai locali / armadi dove sono gestiti archivi cartacei è controllato e selezionato.
Errore materiale (eventi relativi ai comportamenti)	Eventi legati ad errori nella gestione	medio basso	definizione di regole per la gestione delle risorse informatiche;
			definizione di regole per la gestione di dati personali su supporti cartacei;
			sorveglianza sulle attività lavorative degli incaricati;

	informatica o cartacea di dati personali che possono generare la loro perdità di integrità e riservatezza dei dati		simulazioni di crash test.
Comportamenti sleali o fraudolenti (eventi relativi ai comportamenti degli operatori)	Comportamenti dei dipendenti che possono generare distruzione, perdita di integrità e riservatezza dei dati	basso	sorveglianza sulle attività lavorative degli incaricati;
			attivazione di azioni disciplinari verso i dipendenti che si siano resi colpevoli di comportamenti sleali verso l'azienda;
			rispetto del codice etico.
Intercettazioni di informazioni in rete (eventi relativi agli strumenti)	Accesso via rete ai dati personali gestiti su supporti informatici	basso	presenza di firewall a protezione della rete interna.
Malfunzionamento indisponibilità o degrado degli strumenti (eventi relativi agli strumenti)	Indisponibilità o degrado degli strumenti	basso	attivazione di un servizio di assistenza periodica per la verifica del corretto funzionamento dei dispositivi.
Azione di virus informatici o di programmi suscettibili di recare danno (eventi relativi agli strumenti)	Danneggiamento degli strumenti elettronici e delle basi dati contenenti dati personali	medio alto	presenza di strumenti antivirus sul PC collegato in rete;
			attivazione di firewall a protezione dell'accesso in rete pubblica internet;
			aggiornamento periodico dei PC, server e dei sistemi informativi con patch di sicurezza;
			aggiornamento periodico dei dispositivi antivirus;
			istruzioni agli incaricati di controllare qualsiasi supporto di provenienza sospetta prima di operare su uno qualunque dei file in esso contenuti.
Accessi esterni non autorizzati (eventi relativi al contesto fisico ambientale)	Accesso esterno non autorizzato ai dati personali	basso	definizione da parte del responsabile della sicurezza informatica di regole per l'accesso ai locali;
			l'accesso agli incaricati e agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
			l'accesso ai locali dove sono gestiti archivi cartacei è controllato e selezionato;
			tutte le operazioni di manutenzione sono effettuate on site e avvengono con la supervisione dell'incaricato del trattamento o suo delegato;
			divieto di installazione di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.
Accessi non autorizzati a locali ad accesso ristretto (eventi relativi al contesto fisico ambientale)	ingressi non autorizzati ai locali ad accesso ristretto	medio	controllo o sorveglianza da parte dei responsabili;
			porta chiusa per l'accesso all'area in cui sono custoditi i server;
			i server sono in locali chiusi a chiave con impianto di climatizzazione protetti da password sia di rete che di sistema;
			archivi cartacei custoditi in armadi chiusi;
			l'accesso ai locali può avvenire esclusivamente durante l'orario di lavoro e fuori dell'orario solo con autorizzazione del responsabile.
Asportazione e furto di strumenti contenenti dati (eventi relativi al contesto fisico ambientale)	asportazione e furto di strumenti contenenti dati	basso	locali con porte chiuse;
			i backup sono custoditi in locali e archivi ad accesso controllato e sicuro;
			i backup sono realizzati con frequenza giornaliera, settimanale e mensile e identificati;
Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria (eventi relativi al contesto fisico ambientale)	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	basso	gestione delle misure di sicurezza previste dal Testo Unico Sicurezza Lavoro D.lgs. 81/2008 e s.m.;
			adozione delle misure previste dalla normativa antincendi;
			impianto di condizionamento per la gestione dell'areazione dei locali;
			periodicamente ogni sei mesi viene verificato il livello di sicurezza dei siti.

Rischi legati agli strumenti impiegati nei trattamenti

Sono state individuate come sorgenti soggette a rischio le seguenti categorie:

	Fattori di rischio	
Strumenti impiegati	**contesto fisico ambientale**	**comportamento degli operatori**
Schedari ed altri supporti cartacei custoditi nell'area controllata	BASSO	MEDIO
Elaboratori non in rete costoditi nell'area controllata	BASSO	MEDIO
Elaboratori in rete internet	BASSO	MEDIO

Per quanto riguarda il contesto fisico ambientale, la tipologia delle attività e l'adozione di opportune misure tecnico organizzative minimizzano i rischi.

Per il comportamento degli operatori, l'Istituto intende minimizzare il rischio di comportamenti fraudolenti da parte degli operatori, attraverso un'azione di sensibilizzazione degli stessi verso comportamenti rispondenti alle politiche aziendali e al rispetto dei diritti dell'interessato.

Per quanto riguarda gli strumenti informatici l'adozione di mezzi in linea con l'evoluzione tecnologica e l'utilizzo di strumenti, tecniche e policy di sicurezza che garantiscono la minimizzazione dei rischi di perdita, riservatezza, integrità dei dati e distruzione degli stessi.

Gestione delle vulnerabilità rilevate

Non sono state rilevate particolari criticità per quanto riguarda la gestione degli eventi di rischio del sistema informativo. In particolare, per le aree di maggior rischio, relative all'accesso banche dati dell'Istituto da parte di utenti esterni, l'utilizzo di dispositivi firewall minimizza il rischio. Per quanto riguarda i computer in rete, sono attivate le necessarie procedure per la gestione dell'accesso controllato ai sistemi attraverso l'utilizzo di codici identificativi utente e parole chiave.

Le attività di trattamento dei dati sono realizzate sotto sorveglianza del responsabile che supervisiona l'effettiva applicazione degli adempimenti a tutela della privacy.

Per la gestione di dati sensibili, l'Istituto intende minimizzare la loro presenza ed effettuare la gestione di quelli strettamente necessari secondo logiche di accesso controllato ovvero attraverso l'utilizzo di codici identificativi utente e parole chiave di accesso alle banche dati informatizzate e gestione di procedure di accesso selezionato e controllato per quelle di tipo cartaceo.

Misure atte a garantire l'integrità e disponibilità dei dati

- Protezione di aree e locali dove sono contenuti dati personali
  - locali condizionati e opportunamente aerati;
  - accesso ai locali esclusivamente durante l'orario di lavoro e controllato;
  - locali server con porta chiusa e condizionamento interno;
  - verifica periodica semestrale del livello di sicurezza dei siti;
  - gestione delle misure di sicurezza previste dal D.lgs. 626/94 e antincendio;
- Custodia e archiviazione dei dati
  - istruzioni agli incaricati per la custodia in luogo sicuro delle credenziali;
  - esecuzione di backup con cadenza giornaliera, settimanale e mensile per i sistemi che contengono dati personali;
  - conservazione dei backup in locali diversi da quelli dove sono locati gli archivi di gestione.
- Misure logiche di sicurezza
  - sussistenza delle condizioni per le quali l'incaricato gode dei profili di autorizzazione;
  - sistema di autenticazione informatica al fine di accertare l'identità degli incaricati che accedono agli strumenti elettronici;
  - accesso ai server protetto da password di rete e di sistema;
  - definizione di regole per la gestione di dati personali su supporti cartacei;
  - definizione di regole per la gestione sicura di password;
  - accesso ai sistemi informatici tramite rete internet protetta da firewall;
  - modifica della propria password ogni 6 mesi per l'accesso ai dati personali e 3 mesi per l'accesso ai dati sensibili;
  - codice identificativi personali disattivati in caso di mancato utilizzo per più di 6 mase;
  - adozione di procedure di monitoraggio delle utenze;
  - definizione di regole per la gestione delle risorse informatiche ed elettroniche da parte degli incaricati.
- Accesso ai dati e istruzioni impartite agli incaricati
  - comunicazione delle regole per la definizione sicura di password;

- attivazione di azioni di formazione sulle tematiche di sicurezza dati;
- istruzioni per la custodia e utilizzo dei supporti rimovibili contenenti dati personali e controllo dei supporti di provenienza sospetta prima di qualsiasi operazione;
- istruzioni per la gestione di dati personali con strumenti elettronici e cartacei;
- ogni incaricato è dotato di codice identificativo e parola chiave univoci e personali, costituenti le sue credenziali di autenticazione;
- definizione delle tipologie di dati ai quali gli incaricati possono accedere;
- divieto di lasciare incustodito o accessibile gli strumenti elettronici;
- divieto di memorizzare dati personali sui computer.

- Protezione di strumenti e dati
  - gestione e aggiornamento dell'elenco dei portatili assegnati agli utenti con l'indicazione dei dati che possono essere memorizzati;
  - simulazioni di crash test;
  - strumenti antivirus sui computer collegati alla rete interna;
  - sistema centralizzato d'invio e aggiornamento ai client dell'antivirus;
  - aggiornamento dei computer e dei server con patch di sicurezza;
  - attivazione di firewall a protezione dell'accesso alla rete interna;
  - controllo sulle mail e allegati con strumenti antivirus e malware;
  - restore delle banche dati, a partire dai backup a fronte di distruzione o perdita di dati;
  - le operazioni di manutenzione sono autorizzate e avvengono sotto la supervisione dell'incaricato. Gli accessi da remoto sono autorizzati e consentiti solo attraverso un canale protetto da firewall.

Criteri e modalità di ripristino dei dati

Per i dati trattati con strumenti elettronici sono previste procedure di backup attraverso le quali le informazioni vengono memorizzate e salvate giornalmente, settimanalmente e mensilmente su supporti magnetici residenti su unità di backup localizzate in ambienti diversi da quello di origine.

Le copie di salvataggio sono utilizzate in caso di perdita o distruzione dei dati di origine. Sono pianificate prove annuali di ripristino per la verifica della consistenza delle copie di salvataggio.

Affidamento di trattamenti di dati personali all'esterno

La responsabilità del trattamento dei dati personali affidato all'esterno è del titolare del trattamento, che individua il responsabile esterno. Tra il titolare ed il responsabile esterno si deve stipulare regolare contratto al fine di garantire quanto stabilito dal Regolamento (UE) 2016/679 per la protezione dei diritti e le libertà fondamentali delle persone fisiche.

Controllo generale sullo stato della sicurezza

Il titolare del trattamento dei dati mette in atto misure tecniche e organizzative tali per garantire ed essere in grado di dimostrare che il trattamento è conforme al Regolamento (UE) 2016/679 e ne verifica l'efficacia regolarmente.

In particolare per gli archivi cartacei rispetto a:

- procedure di archiviazione e custodia dei dati personali;
- accesso fisico ai locali dove si svolge il trattamento;
- rispetto dei principi applicabili al trattamento compreso la sicurezza e la protezione;
- analisi e controllo dei rischi di perdita e distruzione dei dati.

Per gli archivi informatizzati l'adozione delle misure minime di sicurezza ICT per la pubbliche amministrazioni definite dall'Agenzia per l'Italia Digitale con circolare 18 aprile 2017 n. 2/2017 da attuare entro il 31 dicembre 2017.

Allegato 2

Responsabili Interni del trattamento dei dati (Art. 28 Regolamento UE 2016/679)

STRUTTURA	RESPONSABILE
Area Tematica Igiene degli allevamenti	Dr. Antonio Fagiolo
Area Tematica Sanità Animale	Dr. Giancarlo Ferrari
D.O. Accettazione centralizzata	Dr. Francesco Scholl
D.O. Biotecnologie	Dr. Gian Luca Autorino
D.O. Chimica	Dr. Bruno Neri
D.O. Controllo degli Alimenti	Dr. Stefano Bilei
D.O. Controllo Igiene, produzione e trasf. latte	Dr.ssa Simonetta Amatiste
D.O. Diagnosi delle Malattie Virali e delle Leptospirosi	Dr. Gian Luca Autorino
D.O. Diagnostica	Antonio Battisti
D.O. Produzioni Zootecniche	Dr.ssa Olga Lai
Direzione Acquisizione beni e servizi	Dr.ssa Silvia Pezzotti
Direzione Economico-finanziaria	Dr.ssa Silvia Pezzotti
Direzione Gestione risorse umane	Dr. Paolo Nicita
Direzione Tecnica Patrimoniale	Arch. Claudio Scalia
Osservatorio Epidemiologico	Dr.ssa Paola Scaramozzino
Ricerca, Sviluppo e collaborazione internazionale	Dr. Romano Zilli
Sezione Arezzo	Dr. Dario Deni
Sezione Firenze	Dr. Giovanni Brajon
Sezione Grosseto	Dr. Alberigo Nardi
Sezione Latina	Dr. Remo Rosati
Sezione Pisa	Dr.ssa Marcella Guarducci
Sezione Rieti	Dr. Pietro Calderini
Sezione Siena	Dr. Massimo Mari
Sezione Viterbo	Dr. Luigi De Grossi
Sierologia	Dr.ssa Gladia Macrì
Struttura Prevenzione e Protezione	Dr.ssa Silvana Guzzo
Ufficio Controllo di Gestione	Dr. Romano Zilli
Ufficio di Supporto Direzione Generale	Dr. Francesco Filippetti
Ufficio Formazione, comunicazione e documentazione	Dr.ssa Antonella Bozzano
Ufficio Qualità	Dr.ssa Silvana Guzzo

Allegato 3

Responsabili Esterni del trattamento dei dati (Art. 28 Regolamento UE 2016/679)

SOGGETTI ESTERNI	N. DELIBERA DG	OGGETTO DELIBERA
ESG SERVICES S.r.l.	160/2017	Servizio di assistenza tecnica software AS400 – CESSIONE CONTRATTO in favore della ditta ESG SERVICES S.r.l.
New Genesys S.r.l	295/2018	Contratto di manutenzione ordinaria del sistema N-SIL - AGGIUDICAZIONE GARA ed affidamento in favore della ditta New Genesys srl
Oslo S.r.l.	392/2018	Contratto di manutenzione ordinaria, evolutiva ed assistenza del sistema Rcubo affidamento in favore della ditta Oslo srl
INAZ S.r.l.	122/2017	Rinnovo del canone del software INAZ
MAGGIOLI SpA-Divisione ELDASOFT	304/2017	AGGIUDICAZIONE GARA ed affidamento della fornitura in favore della ditta MAGGIOLI SpA-Divisione ELDASOFT
Althea Italia S.p.A	608/2018	Presa d'atto fusione per incorporazione di Elettronica Bio Medicale S.p.A., aggiudicataria per anni quattro della gestione del servizio di manutenzione delle apparecchiature elettromedicali e di laboratorio in A.T.I. con la S.I.E.M. s.a.s., in Althea Italia S.p.A..
Banca Popolare dell'Emilia Romagna Società Cooperativa	167/2016	Procedura aperta di rilevanza comunitaria ex D.lgs 163/06, art. 55, per l'affidamento per anni 3 del servizio di tesoreria dell'Istituto - CIG 6472270E27 – EFFICACIA AGGIUDICAZIONE DEFINITIVA in favore della Banca Popolare dell'Emilia Romagna Società Cooperativa
Dott. Romeo Pulsoni	124/2017	Adesione alla Convenzione Consip "Gestione integrata della salute e sicurezza sui luoghi di lavoro" edizione 3 – Lotto 3 CIG derivato 6901127E25, Lotto 4 CIG derivato 6901300CE9 - NOMINA MEDICO COMPETENTE E MEDICO COORDINATORE