DOCUMENTO DI VALUTAZIONE E GESTIONE DEL RISCHIO PRIVACY©

Approvato dal Consiglio di Amministrazione il 30 ottobre 2018

Procedure di Gestione del Rischio Privacy

REDATTE AI SENSI E PER GLI EFFETTI DEL REGOLAMENTO EUROPEO PRIVACY UE/2016/679 (GDPR)

Il Presente documento di n. 87 pagine (esclusa la copertina), redatto in un'unica copia originale, ha lo scopo di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato dall'azienda qui di seguito identificata (nel seguito del documento indicato come Titolare). Gli artt. 24 e 25 del Regolamento Europeo 2016/679 del 27 aprile 2016 ed il numero 74 dei considerando, entrato in vigore il 25 maggio 2018 (di seguito "Regolamento") prevedono l'obbligo in capo al titolare del trattamento di effettuare una valutazione dei possibili rischi e delle misure attuate per prevenire e/o contrastare tali rischi.

In precedenza la Titolare aveva adempiuto a simili adempimenti, redigendo le Misure Minime di Sicurezza previste dal D.lgs. 196/2003, documento poi abrogato dall'art. 45 del D.L. 9/2/2012 n. 5; l'abrogazione di tale documento non faceva comunque venir meno l'obbligo di osservare e documentare le misure di sicurezza attuate e quelle programmate per contrastare e/o prevenire i rischi in materia di trattamento di dati personali, cosicché lo studio aveva comunque redatto un documento in merito.

Con il presente documento si intende quindi aggiornare e sostituire quelli precedenti, tenendo presente che, ai fini della valutazione del rischio, viene ritenuto indispensabile fare riferimento agli accadimenti e ad eventuali rischi verificatisi in precedenza. Al di là delle disposizioni recate dal Regolamento, tenuto conto dell'obbligo di riservatezza, si reputa siano da tutelare sia i dati definiti "particolari" dall'art. 9 del Regolamento (ex dati definiti "sensibili" dal D.lgs. 196/2003) sia i dati economici, patrimoniali e reddituali dei clienti e fornitori dalla Titolare, anche dei soggetti non interessati dal Regolamento, rammentando che le disposizioni in materia di tutela dei dati personali sono applicabili unicamente alle persone fisiche (art. 1 del Regolamento).

Non da ultimo, giova sottolineare, che il documento tiene particolare conto di tutti i quei dati gestisti che, seppur irrilevanti ai fini del vigente GDPR, la loro perdita o uso improprio, potrebbe essere suscettibile di causare gravi danni economici e patrimoniali, nonché di immagine alla Titolare.

Il presente documento deve essere custodito in idonee condizioni di sicurezza in azienda e deve essere esibito agli organi di controllo competenti. Il documento è strutturato in paragrafi in cui il testo riportato in carattere normale rappresenta quanto indicato dal Garante per assicurazione la gestione del sistema privacy secondo il principio dell'accountability e nelle relative istruzioni operative, mentre in corsivo viene riportato quanto effettivamente applicato dalla Fondazione. Si precisa che, nella redazione del presente documento si è preso atto delle più recenti disposizioni del Garante della Privacy, e, in particolare:

- **Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche – 2 luglio 2015**
- **Lavoro: le linee guida del Garante per posta elettronica e internet Gazzetta Ufficiale n. 58 del 10 marzo 2007**
- **Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679**
- **Linee guida sul diritto alla portabilità dei dati e sui responsabili della protezione dei dati**
- **Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento– Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"**

Ragione sociale	***FONDAZIONE APULIA FILM COMMISSION***
	ISCRITTA AL NR. 52/P DEL REGISTRO DELLE PERSONE GIURIDICHE
Fondo di dotazione	***€ 50,000*** *capitale versato:* ////
Sede legale in	***Bari*** *Via* ***L.re Starita 1 Pad. 180 – F.d.L.***
Partita IVA	**06631230726** *Codice fiscale e reg. impresa* **93332290720**
CCIAA di	***Bari*** *REA n.* ***500449***
rappresentata dal Dott.	***Sciarra Maurizio***
In qualità di	***Presidente del C.d.A.***

Il presente Documento, che sostituisce i precedenti in vigore, ripartendo dalla revisione 10, viene redatto per fornire alle autorità di controllo evidenza oggettiva dell'impegno aziendale teso a tutelare i dati personali e i dati aziendali di qualsiasi natura gestita; il presente sistema di gestione del rischio Privacy è perfettamente integrato al Modello di Organizzazione e Gestione dei Rischi redatto ai sensi del Dlgs 231/2001 adottato dalla Titolare:

INDICE

0	**Descrizione azienda**	**pag.**	**5**
	0.1 Organigramma funzionale	"	6
	0.2 Stato delle revisioni	"	8
1	**L'elenco dei trattamenti dei dati personali**	**"**	**9**
	1.1 Tipologie di dati trattati	"	9
	1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano	"	13
	1.2.1 La mappa dei Sistemi di elaborazione	"	16
	1.3 La mappa dei trattamenti effettuati	"	34
2	**Mansionario privacy ed interventi formativi degli incaricati**	**"**	**37**
	2.1 I Responsabili del trattamento	"	38
	2.2 Il Responsabile delle misure minime di sicurezza	"	40
	2.3 Il Responsabile per garantire il soddisfacimento dei diritti esercitabili dai soggetti interessati	"	42
	2.4 Predisposizione e aggiornamento mansionario privacy	"	46
	2.5 Pianificazione degli interventi formativi degli incaricati e del personale preposto	"	47
	2.5.1. Tabella: pianificazione degli interventi formativi previsti	"	49
	2.6 Organigramma nominativo "Privacy"	"	50
3	**Analisi dei rischi che incombono sui dati**	**"**	**51**
4	**Misure atte a garantire l'integrità e la disponibilità dei dati**	**"**	**57**
	4.1 La protezione di aree e locali	"	57
	4.2 La custodia e l'archiviazione di atti, documenti e supporti	"	58
	4.2.1 Affidamento degli incarichi e la custodia di atti e documenti	"	58
	4.2.2 Archiviazione di atti e documenti	"	58
	4.3 Le misure logiche di sicurezza	"	60
	4.4 Adozione di un sistema di autenticazione informatica	"	60
	4.5 Adozione di un sistema di autorizzazione	"	64
5	**Criteri e modalità di ripristino dei dati**	**"**	**65**
6	**L'affidamento di dati personali all'esterno**	**"**	**69**
	6.1 Tabella : trattamenti affidati all'esterno	"	71
7	**Controllo generale sullo stato della sicurezza "Data Breach e procedure di continuità operativa**	**"**	**72**
8	**Valutazione di impatto sulla protezione dei dati "DPIA e Registro dei trattamenti**	**"**	**79**
9	**Dichiarazione di impegno e firma**	**"**	**82**
all. A	**Tabella di supporto al paragrafo 1**	**"**	**83**

0 DESCRIZIONE DELL'AZIENDA

La Fondazione Apulia Film Commission nasce a Bari nel 2007, con l'obiettivo di attrarre le produzioni audiovisive grazie alla competitività dei servizi, alla professionalità delle maestranze e all'abbattimento dei costi di trasferta, cast, troupe e location scouting del territorio, promuovendo e valorizzando il patrimonio artistico e ambientale della Puglia e del Mediterraneo in Italia e all'estero.

La Fondazione annovera tra i **soci** 33 tra Province e Comuni pugliesi, ed è iscritta nel Repertorio Economico e amministrativo della Camera di commercio di Bari e al registro delle persone giuridiche tenuto dalla Prefettura competente.

Nel 2010, la Fondazione inaugura la sua nuova e attuale sede legale e operativa conosciuta come "Cineporto di Bari": un padiglione all'interno della Fiera del Levante di 1200 mq di superficie interamente dedicata al cinema e alle arti visive dotato di una serie di servizi nel campo della produzione cinematografica e della comunicazione in genere.

La Fondazione Apulia Film Commission annovera tra i **soci** 33 tra Province e Comuni pugliesi, presieduta da **Maurizio Sciarra**, fa parte di Cine-Regio, network europeo di Fondi regionali per l'audiovisivo, della AFCI – Associazione delle Film Commission mondiali, del coordinamento delle film commission italiane (IFC), alla EUFCN, della Conferenza permanente per l'audiovisivo del mediterraneo (COPEAM) e partecipa stabilmente ai tavoli ministeriali di concertazione delle politiche di settore.

La Fondazione promuove lo sviluppo della cultura cinematografica nel territorio regionale e il sostegno all'industria audiovisiva attraverso il **"Centro Studi, formazione e ricerca sul cinema e l'audiovisivo"**, nato per favorire le attività formative, il networking scientifico e lo stimolo ai film studies, realizzati in collaborazione con le Università e i centri di eccellenza regionali.

Ad Apulia Film Commission fa capo anche la **Mediateca regionale pugliese** di Bari, destinata a diventare insieme ai tre Cineporti di Puglia, il polo della formazione e della ricerca per i futuri cineasti e per i cittadini pugliesi.

Apulia Film Commission sostiene e finanzia progetti trasversali realizzati grazie alle politiche culturali della Regione Puglia con l'ausilio dei Fondi Strutturali Europei. Negli obiettivi europei c'è la Rete dei festival, rassegne internazionali come il **Bi&fest** e la **Festa di cinema del Reale** di Specchia (Le). Senza dimenticare l'attenzione al pubblico, la programmazione di ben 21 sale attraverso il **Circuito d'Autore**, una rete di cinema in cui la programmazione è al 51% di film italiani e europei accanto a prospettive e rassegne d'autore a fronte di un contributo annuale di 36mila euro oltre IVA a ciascuna sala.

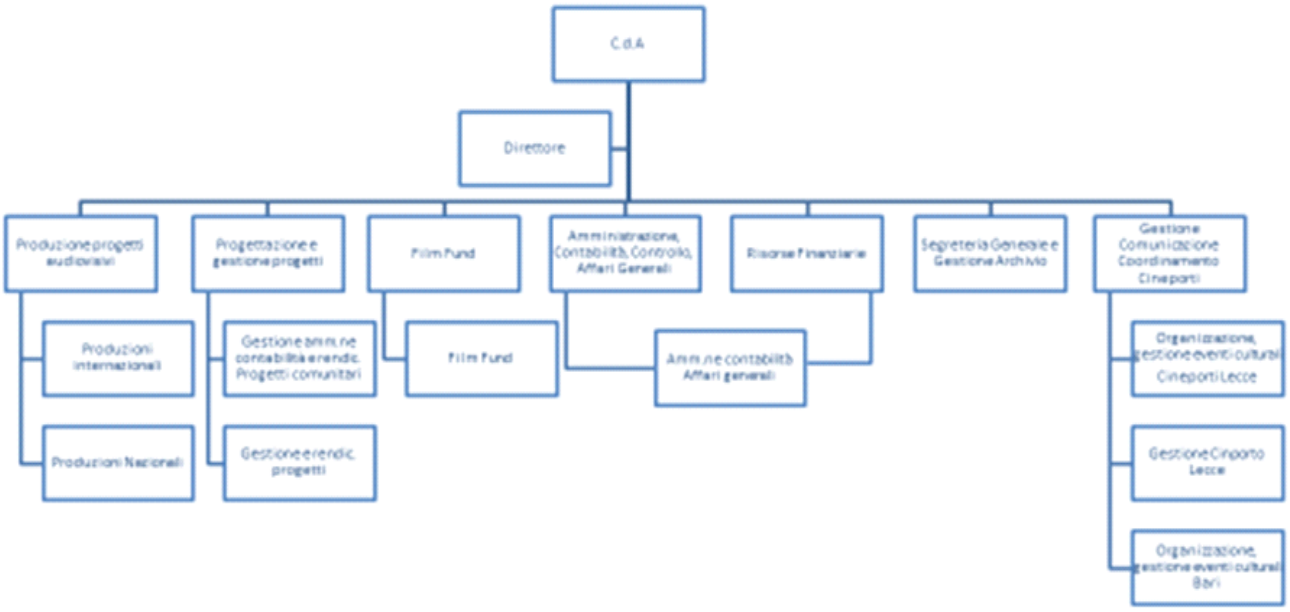
Elenco sedi periferiche:

Cineporto di Puglia Sede di Lecce Via Vecchia Frigo – 73100 Lecce

Cineporto di Puglia Sede di Foggia Via San Severo, KM 2,00 - 71121 Foggia

Mediateca Regionale Puglia– Via Giuseppe Zanardelli 30 – 70125 Bari

0.1 ORGANIGRAMMA FUNZIONALE



0.2 STATO DELLE REVISIONI

TABELLA DELLE REVISIONI

Capitolo	REV. **0**	REV. **1**	REV. **2**	REV. **3**	REV. **4**	REV. **5**	REV. **6**	REV. **7**	REV. **8**	REV. **9**	REV. **10**
Manuale	*Data*	*Data*	*Data*	*Data*	*Data*	*Data*	*Data*	*Data*	*Data*	*Data*	*Data*
Cap.0	*30/03/2008*	*31/03/2009*	*23/03/2010*	*29/03/2011*	*29/03/2012*	*29/03/2013*	*28/03/2014*	*31/03/2015*	*31/03/2016*	*31/03/2017*	*30/10/2018*
Cap.1	*30/03/2008*	*31/03/2009*	*23/03/2010*	*29/03/2011*	*29/03/2012*	*29/03/2013*	*28/03/2014*	*31/03/2015*	*31/03/2016*	*31/03/2017*	*30/10/2018*
Cap.2	*30/03/2008*	*31/03/2009*	*23/03/2010*	*29/03/2011*	*29/03/2012*	*29/03/2013*	*28/03/2014*	*31/03/2015*	*31/03/2016*	*31/03/2017*	*30/10/2018*
Cap.3	*30/03/2008*	*31/03/2009*	*23/03/2010*	*29/03/2011*	*29/03/2012*	*29/03/2013*	*28/03/2014*	*31/03/2015*	*31/03/2016*	*31/03/2017*	*30/10/2018*
Cap.4	*30/03/2008*	*31/03/2009*	*23/03/2010*	*29/03/2011*	*29/03/2012*	*29/03/2013*	*28/03/2014*	*31/03/2015*	*31/03/2016*	*31/03/2017*	*30/10/2018*
Cap.5	*30/03/2008*	*31/03/2009*	*23/03/2010*	*29/03/2011*	*29/03/2012*	*29/03/2013*	*28/03/2014*	*31/03/2015*	*31/03/2016*	*31/03/2017*	*30/10/2018*
Cap.6	*30/03/2008*	*31/03/2009*	*23/03/2010*	*29/03/2011*	*29/03/2012*	*29/03/2013*	*28/03/2014*	*31/03/2015*	*31/03/2016*	*31/03/2017*	*30/10/2018*
Cap.7	*30/03/2008*	*31/03/2009*	*23/03/2010*	*29/03/2011*	*29/03/2012*	*29/03/2013*	*28/03/2014*	*31/03/2015*	*31/03/2016*	*31/03/2017*	*30/10/2018*
Cap.8	*30/03/2008*	*31/03/2009*	*23/03/2010*	*29/03/2011*	*29/03/2012*	*29/03/2013*	*28/03/2014*	*31/03/2015*	*31/03/2016*	*31/03/2017*	*30/10/2018*
Procedura 1											*30/10/2018*
Procedura 2											*30/10/2018*
Procedura 3											*30/10/2018*
Procedura 4											*30/10/2018*
Procedura 5											*30/10/2018*

1. L'ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

*Per **"trattamento"***, si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

1.1 TIPOLOGIE DI DATI TRATTATI

I dati il cui trattamento giustifica l'esistenza di un sistema di protezione dati basato sulle evidenze oggettive sono principalmente "dati personali".

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

Particolarmente importanti sono:

• i **dati comuni** che permettono l'**identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

• i **dati** rientranti in **particolari** categorie: si tratta dei dati c.d**. "sensibili**", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute, alla vita o all'orientamento sessuale; il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i **dati "genetici"** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione, inclusivi anche dei dati relativi alla salute dell'individuo, e i **dati "biometrici",** i 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;

• **i dati relativi a condanne penali e reati**: si tratta dei dati c.d. **"giudiziari",** cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

= = . = =

Nell'esercizio delle sue attività la Titolare, nella sede legale di Bari, Lecce e Foggia, nonché presso la Mediateca Regionale, procede al trattamento di dati diversi da quelli particolari e giudiziari, ovvero solo dati comuni, relativi a soggetti diversi, come meglio specificato nella Tabella di supporto allegata alla presente procedura.

La Titolare, gestisce esclusivamente dati comuni in relazione all'attività specifica svolta, e demanda una serie di adempimento ad una serie di professionisti diversi.

Di seguito si riporta l'individuazione delle macroclassi di dati trattati, con particolare riferimento ai processi aziendali:

1. ***Dati comuni relativi alla tenuta della contabilità aziendale**, **cod. 01**: trattasi principalmente di dati in forma cartacea ed elettronica relativi alla traduzione da linguaggio analogico a quello contabile di tutte le operazioni aziendali necessarie per adempiere a imposizioni di carattere civilistico e fiscale: anagrafiche clienti/fornitori, fatture, documentazione fiscale e contabile, buste paga, contratti, preventivi, documentazione legale, agenti e rappresentanti;*
2. ***Dati relativi al personale dipendente**, **o ad eventuali potenziali candidati aspiranti a borse di studio, stage**, **cod. 02**: trattasi principalmente di dati in forma*

cartacea ed elettronica finalizzati all'esecuzione di adempimenti lavoristico-previdenziali, alla composizione delle schede valutative dei dipendenti, gestione curriculum, elaborazione del costo del lavoro per la formazione delle buste paga, certificati medici, stati di famiglia, ecc.;

3. ***Dati comuni relativi al servizio espletato cod. 03**, trattasi principalmente di una serie di dati in forma cartacea ed elettronica, che vengono trattati per i fini prettamente istituzionale dell'Ente, ivi inclusi quelli custoditi nel proprio sito internet www.apuliafilmcommission.it: gli stessi vengono divisi in sottoclassi come segue:*
   - ***03A - Progettazione e Gestione Progetti (Cineporto Bari);***
   - ***03B –Produzioni e progetti audiovisivi (Cineporti Bari, Lecce e Foggia);***
   - ***03C –Film Fund (Cineporto Bari) – in qualità di Responsabile del Trattamento;***
   - ***03D – Cineporti (Cineporti Bari, Lecce e Foggia);***
   - ***03E – Mediateca (presso la sede indicata) in qualità di Responsabile del Trattamento**;*
4. *Altri tipi di Dati relativi a vari soggetti **cod. 04**: trattasi principalmente di dati in forma cartacea ed elettronica relativi a soggetti che entrano in contatto non sistematico con l'organizzazione, e di altra documentazione non classificabile negli altri codici sopra indicati (a titolo meramente esemplificativo ma non esaustivo: agende di vario tipo, biglietti da visita, mailing lists, appunti, documentazione legale,ecc.*

Nelle Unità locali di Lecce e Foggia, nonché nella Mediateca Regionale di Bari, sono custoditi trattati dati afferenti ai codici 03 e 04, ristretti al minimo indispensabili anche perché tutta la documentazione elettronica è localizzata in un server fisicamente presente presso la sede legale, mentre la quasi totalità della documentazione cartacea, subisce solo alcune fasi del trattamento per poi convergere presso la sede legale di Bari.

Si rappresenta, altresì, che con specifico riferimento ai codici 3C e 3E l'Apulia Film Commission svolge le funzioni di gestore del servizio, mentre la Regione Puglia è Titolare del trattamento.

I dati in questione sono meglio specificati nella Tabella A allegata alla presente procedura.

Tabella 1.1: Elenco dei trattamenti: informazioni base

Id. trattamento	*Modalità del trattamento*	*Natura dati*	*Funzioni di riferimento*	*Responsabili Interni*	*Trattamenti affidati esterno*	*Descrizione degli strumenti utilizzati*
Cod. 01	*Elettronico Cartaceo*	*Comuni*	*Amministrazione*	*Parente Antonio – Direttore* *Ciro Attanasio – Resp. Fin.*	*De Vito Ernesto - OdV* *Pierno Ruggiero – Amm, Fisco e Bil.* *Plantone Vito – Contabilità* *HSH Srl – Gestione informatica* *Pierno Riccardo - DPO* *Sigma Sistemi Srl* *Pulisan Srl*	*Sistema Informativo Aziendale* *Fascicoli riposti in schedari, armadi con apposita chiusura*
Cod. 02	*Elettronico Cartaceo*	*Comuni*	*Personale*	*Parente Antonio – Direttore*	*De Vito Ernesto - OdV* *Stefanelli Nicola – RSPP* *Cafagna Eugenio – Medico competente* *Plantone Vito – Contabilità* *Pierno Fabrizio – Consulenza Lavoro* *HSH Srl – Gestione informatica* *Pierno Riccardo – DPO* *HSH Srl – Gestione informatica* *Pulisan Srl* *Temporary SpA*	*Sistema Informativo Aziendale* *Fascicoli riposti in schedari, armadi con apposita chiusura*
Cod. 03	*Elettronico Cartaceo*	*Comuni*	*Contratti, appalti e progettazione*	*Piscitelli Cristina – RUP*	*De Vito Ernesto - OdV* *Pierno Riccardo – DPO* *Palumbo Giuseppe – Legale civile* *Garofalo Domenico – Legale civile* *Patroni Griffi Ugo – Legale civile* *Cartolano Roberto – Legale ammin.vo* *Persichella Sabino – Legale ammin.vo* *HSH Srl – Gestione informatica* *Pulisan Srl*	*Sistema Informativo Aziendale* *Fascicoli riposti in schedari, armadi con apposita chiusura*
			Produzioni	*Basilio Daniele*	*De Vito Ernesto - OdV* *Pierno Riccardo – DPO* *HSH Srl – Gestione informatica* *Pulisan Srl*	
			Film Fund	*Regione Puglia (Titolare)* *Corciulo Roberto (Responsabile)*	*De Vito Ernesto - OdV* *Pierno Riccardo – DPO* *HSH Srl – Gestione informatica* *Pulisan Srl*	
			Cineporti	*Parente Antonio – Direttore*	*De Vito Ernesto - OdV* *Pierno Riccardo – DPO* *HSH Srl – Gestione informatica* *Pulisan Srl*	
			Mediateca	*Regione Puglia (titolare)* *Parente Antonio – Direttore*	*De Vito Ernesto – OdV* *Pierno Riccardo – DPO* *HSH Srl – Gestione informatica* *Pulisan Srl*	
Cod. 04	*Elettronico Cartaceo*	*Comuni*	*Amministrazione & Personale*	*Parente Antonio – Direttore*	*De Vito Ernesto – OdV* *Pierno Ruggiero – Amministrazione* *Plantone Vito – Contabilità* *HSH Srl – Gestione informatica* *Pierno Riccardo – DPO* *HSH Srl – Gestione informatica* *Pulisan Srl*	*Sistema Informativo Aziendale* *Fascicoli riposti in schedari, armadi con apposita chiusura*

1.2 CARATTERISTICHE DI AREE, LOCALI E STRUMENTI CON CUI SI EFFETTUANO I TRATTAMENTI

Il nuovo codice mantiene la distinzione di fondo, già presente nel Dpr 318/1999, tra trattamenti effettuati con:

- strumenti **elettronici**, termine nel quale la lettera b) del comma 3 dell'articolo 4 fa rientrare gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- strumenti **diversi da quelli elettronici**: agendine in cui sono annotati nomi, pesanti raccoglitori nei quali sono racchiuse pratiche, schedari da non aprire in condizioni di corrente ventosa, nonché simili, e tuttora assai diffusi nonostante si sia in piena rivoluzione *virtuale*, mezzi tradizionali di annotazione, conservazione e consultazione di informazioni e dati.

Al fine di disciplinare le misure di sicurezza, il precedente Dpr 318/1999 *distingueva nettamente*, nell'ambito degli strumenti elettronici, quelli:

- **non in rete**, cioè non accessibili da altri elaboratori, terminali o, più in generale, da altri strumenti elettronici;
- accessibili, da altri elaboratori o più in generale da altri strumenti elettronici, solo attraverso **reti non disponibili al pubblico**: è il caso ad esempio di una rete aziendale, che ha solo collegamenti interni via cavo;
- accessibili mediante una **rete** di telecomunicazioni **disponibile al pubblico**.

N.B.

Alla luce di questa classificazione, erano sorte alcune incertezze, in merito alla circostanza che uno strumento elettronico potesse, o meno, essere considerato essere *in rete*, e se questa fosse *privata* (cioè non disponibile al pubblico) o *pubblica*. A tale riguardo, la relazione di accompagnamento al Dpr 318/1999 ha spiegato che "la distinzione si fonda sulla utilizzazione o meno, per la comunicazione, di reti di comunicazione disponibili al pubblico: essa, a livello di prima approssimazione, riguarda da un lato i sistemi che utilizzano una rete proprietaria, sulla quale possono viaggiare unicamente i dati del titolare del sistema, e dall'altro gli elaboratori che utilizzano *anche solo per alcuni tratti* reti di telecomunicazione disponibili al pubblico. In quest'ottica, vengono a rientrare in questa seconda categoria anche le reti cosiddette geografiche, quando l'interconnessione tra sistemi non accessibili al pubblico venga effettuata mediante una tratta, anche se limitata, di rete pubblica".

La relazione proseguiva spiegando che "la distinzione trova il suo fondamento nel diverso livello di

rischio, conseguente alla utilizzazione di un mezzo di trasporto dei dati comunque accessibile anche da parte di altri soggetti: in caso di condivisione di un identico tratto di linea telefonica, anche se i dati viaggiano separati, la possibilità di accesso è infatti sicuramente più semplice, rispetto ad un sistema di interconnessione autonomo, nel quale viaggiano unicamente i dati del titolare".

Sulla base di queste considerazioni, si è dovuto concludere che *anche un singolo elaboratore*, che non fosse fisicamente in rete con altri, ma disponesse di modem e di connessione Internet, dovesse essere considerato come *accessibile mediante una rete di telecomunicazioni disponibile al pubblico*, con la conseguenza di dovere applicare ad esso le più severe misure di sicurezza, previste per tale ipotesi, rispetto a quanto stabilito per gli elaboratori non in rete, o collegati tra loro mediante rete privata.

Nel disciplinare tecnico, allegato al nuovo codice, viene a **perdere qualunque rilievo la distinzione**, presente nel precedente Dpr 318/1999, tra trattamenti effettuati con strumenti elettronici non accessibili da altri elaboratori, terminali o in generale strumenti, e trattamenti con strumenti elettronici *accessibili in rete*, e, nell'ambito di questi ultimi, l'ulteriore distinzione tra l'accessibilità attraverso reti disponibili o non disponibili al pubblico. **Per l'utilizzo di tutti gli elaboratori, viene quindi imposta l'adozione delle misure di sicurezza più severe, che in precedenza erano riservate ai soli trattamenti con elaboratori in rete.**

= = . = =

Il trattamento dei dati avviene in particolare presso la sede legale della Titolare all'interno del Ente Fiera del Levante in un padiglione della stessa denominato Cineporto.

La struttura è dotata dei più recenti sistemi d'allarme e antintrusione, tali da limitare i rischi di accessi indesiderati e furti, inclusa la videosorveglianza nelle zone perimetrali; il tutto giustificato dalla tutela e difesa del patrimonio aziendale.

L'ingresso alla struttura è organizzato con una modalità di accesso ***controllato a 2 livelli****:*

1. *identificazione all'ingresso dell'Ente Fiera da parte del personale preposto alla vigilanza, con l'ausilio di un passaggio a livello;*
2. *identificazione all'ingresso della sede a cura degli addetti alla segreteria, con accompagnamento dell'ospite presso l'Area richiesta.*

Il trattamento dei dati personali avviene con i ***seguenti strumenti****:*

A – Schedari ed altri supporti cartacei

I supporti cartacei, ivi inclusi quelli contenenti immagini, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati o

distrutti, una volta terminato il loro esame.

Tutti gli archivi in questione sono localizzati nell'area destinata ad uffici, e sono organizzati con armadi ignifughi di sicurzza.

In particolare, gli stessi sono organizzati come segue:

- *Archivio ad accesso controllato relativo ai Codd. 01, 02, 03A,B,C,D ed E e 04, localizzati nelle rispettive aree di competenza e in un archivio ad accesso controllato ad uso comune da parte delle varie funzioni.*

B – Elaboratori non in rete

Per elaboratori non in rete si intendono quelli non accessibili da altri elaboratori, terminali o, più in generale, da altri strumenti elettronici.

La Titolare non dispone di elaboratori aventi le suddette caratteristiche.

C – Elaboratori in rete privata

Per elaboratori in rete privata si intendono quelli accessibili, da altri elaboratori o più in generale da altri strumenti elettronici, solo attraverso reti proprietarie, sulle quali possono viaggiare unicamente i dati del titolare del sistema.

La Titolare non dispone di elaboratori aventi le suddette caratteristiche.

D – Elaboratori in rete pubblica

Per elaboratori in rete pubblica si intendono quelli che utilizzano, anche solo per alcuni tratti, reti di telecomunicazione disponibili al pubblico, ivi inclusa la rete Internet.

Questa tipologia di apparecchiature meglio descritta nella mappatura di seguito riportata, comprende computer di base fissa e computer portatili consegnati in dotazione ai vari collaboratori in organico alla Titolare.

Allo stato attuale la Titolare dispone di elaboratori aventi le suddette caratteristiche, meglio dettagliati alla lettera D), avendo gli stessi una possibilità autorizzativa ad avvalersi della rete internet (rete pubblica), ma con un solido sistema di settaggio dei profili di accesso.

L'Azienda è altresì dotata di accessi personalizzati e settoriali strettamente legati ai profili autorizzativi assegnati ai singoli utenti.

1.2.1 MAPPA DEI SISTEMI DI ELABORAZIONE

SERV	**Sede**	**Cineporto Bari**
	Ufficio	**Server**
	Incaricato	
	Amministratore sistema	
	Custode password	
	Descrizione	**Rack**
	Modello	**Hp Server**
	Sistema operativo	**Windows Server**
	Impiego	**Server di rete DISMESSO**

Disponibilità

	Stand alone		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus		*Senza antivirus*

SERV	**Sede**	**Cineporto Bari**
	Ufficio	**Server**
	Incaricato	
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**Rack**
	Modello	**Fujitsu Primergy**
	Sistema operativo	**Windows Server 2012**
	Impiego	**Server di rete**

Disponibilità

	Stand alone		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

PRES	**Sede**	**Cineporto**
	Ufficio	**Presidenza**
	Incaricato	**Sciarra Maurizio**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook**
	Sistema operativo	**Mac O.S.**
	Impiego	**Presidenza**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

DIR	**Sede**	**Cineporto Bari**
	Ufficio	**Direzione/Rendicontazione/Progetti EU**
	Incaricato	**Piscitelli Cristina**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook 15" (2012)**
	Sistema operativo	**Mac O.S. 10.6.2**
	Impiego	**Vario**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

AMM	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio/Produzioni**
	Incaricato	**Basilio Daniele**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook 13" (2010)**
	Sistema operativo	**Mac O.S. 10.11**
	Impiego	**Amministrazione**

Disponibilità

[X] *Stand alone* [ ] *In rete non al pubblico* [ ] *In rete pubblica*

Antivurus

[ ] *Con programma antivirus* [X] *Senza antivirus*

Sede	**Cineporto Bari**
Ufficio	**Servizio/Produzioni**
Incaricato	**Fruitore del servizio**
Amministratore sistema	**HSH Informatica & Cultura**
Custode password	
Descrizione	**PC portatile**
Modello	**Macbook 13" (2008)**
Sistema operativo	**Mac O.S. 10.11**
Impiego	**Amministrazione**

Disponibilità

[X] *Stand alone* [ ] *In rete non al pubblico* [ ] *In rete pubblica*

Antivurus

[ ] *Con programma antivirus* [X] *Senza antivirus*

DIR	**Sede**	**Cineporto Bari**
	Ufficio	**Direzione/Amministrativo**
	Incaricato	**Antonio Parente**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC fisso**
	Modello	**iMac 21" (2017)**
	Sistema operativo	**Mac O.S. 10.13**
	Impiego	**Direzione**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

DIR	**Sede**	**Cineporto Bari**
	Ufficio	**Direzione/Amministrativo**
	Incaricato	**Antonio Parente**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook 13" (2017)**
	Sistema operativo	**Mac O.S.**
	Impiego	**Direzione**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

	Con programma antivirus	X	*Senza antivirus*

AMM	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio/Produzioni**
	Incaricato	**Raffaella Del Vecchio**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**MacBook 15" (2012)**
	Sistema operativo	**Mac O.S. 10.12**
	Impiego	**Servizio**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

AMM	**Sede**	**Cineporto Bari**
	Ufficio	**Amministrazione**
	Incaricato	**Fruitore del servizio**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC fisso**
	Modello	**iMac 21" (2011)**
	Sistema operativo	**Mac O.S. 10.13**
	Impiego	**Amministrazione**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

MED	**Sede**	**Mediateca Regionale**
	Ufficio	**Segreteria**
	Incaricato	**Fruitore del servizio**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC fisso**
	Modello	**iMac 27" (2012)**
	Sistema operativo	**Mac O.S. 10.11**
	Impiego	**Segreteria**

Disponibilità

[X] *Stand alone* [ ] *In rete non al pubblico* [ ] *In rete pubblica*

Antivurus

[ ] *Con programma antivirus* [X] *Senza antivirus*

MED	**Sede**	**Mediateca Regionale**
	Ufficio	**Segreteria**
	Incaricato	**Alessandra Aprea**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook 13" (2017)**
	Sistema operativo	**Mac O.S. 10.13**
	Impiego	**Segreteria**

Disponibilità

[X] *Stand alone* [ ] *In rete non al pubblico* [ ] *In rete pubblica*

Antivurus

[ ] *Con programma antivirus* [X] *Senza antivirus*

AMM	**Sede**	**Cineporto Bari**
	Ufficio	**Amministrativo/Produzioni**
	Incaricato	**Massimo Modugno**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**MacBook 15" (2012)**
	Sistema operativo	**Mac O.S. 10.12**
	Impiego	**servizio**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio/Rendicontazione**
	Incaricato	**Andreina De Nicolò**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC fisso**
	Modello	**MacBook iMac 21" (2011)**
	Sistema operativo	**Mac O.S. 10.10**
	Impiego	**Rendicontazione progetti europei**

Disponibilità

	Stand alone		*In rete non al pubblico*	X	*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio/Produzioni**
	Incaricato	**Roberto Corciulo**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**MacBook Pro 15" (2012)**
	Sistema operativo	**Mac O.S. 10.12**
	Impiego	**Film Fund**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio/Rendicontazione**
	Incaricato	**Valeria Corvino**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC fisso**
	Modello	**iMac 20" (2008)**
	Sistema operativo	**Mac O.S. 10.10**
	Impiego	**Rendicontazione progetti europei**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Amministrazione/Finanza**
	Incaricato	**Ciro Alessandro Attanasio**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC fisso**
	Modello	**iMac 20" (2008)**
	Sistema operativo	**Mac O.S. 10.10**
	Impiego	**Amministrazione/Finanza**

Disponibilità

	Stand alone		*In rete non al pubblico*	X	*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Amministrazione/Contabilità**
	Incaricato	**Fruitore del servizio**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC fisso**
	Modello	**iMac 20" (2008)**
	Sistema operativo	**Mac O.S. 10.9**
	Impiego	**Amministrazione/Contabilità**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SEG	**Sede**	**Cineporto Bari**
	Ufficio	**Segreteria**
	Incaricato	**Maria Laurora**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC fisso**
	Modello	**iMac 21" (2009)**
	Sistema operativo	**Mac O.S. 10.10**
	Impiego	**Segreteria**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio/Cineporti**
	Incaricato	**Rocco Colangelo**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC fisso**
	Modello	**iMac 21" (2011)**
	Sistema operativo	**Mac O.S. 10.7**
	Impiego	**Servizi istituzionali/Cineporti**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio**
	Incaricato	**Michele Stella**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**MacBook 15" (2012)**
	Sistema operativo	**Mac O.S. 10.10**
	Impiego	**Servizi istituzionall (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Foggia**
	Ufficio	**Servizio**
	Incaricato	**Pierluigi Del Carmine**
	Amministratore sistema	**HSC Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**MacBook 15" (2012)**
	Sistema operativo	**Mac O.S. 10.13**
	Impiego	**Servizi istituzionall (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio/Comunicazione**
	Incaricato	**Angelo Antonio Cavalluzzi**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**MacBook 13" (2012)**
	Sistema operativo	**Mac O.S.10.13**
	Impiego	**Servizi istituzionall (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio/Cineporti/Proiezioni**
	Incaricato	**Luca Pellicani**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**MacBook 15" (2015)**
	Sistema operativo	**Mac O.S. 10.12**
	Impiego	**Servizi istituzionali (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto**
	Ufficio	**Servizio**
	Incaricato	**D'Oria Serge**
	Amministratore sistema	**HSC Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**MacBook 13" (2017)**
	Sistema operativo	**Mac O.S.**
	Impiego	**Servizi istituzionali (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio/Cineporti/Proiezioni**
	Incaricato	**Fabrizio Stagnani**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**MacBook 15" (2015)**
	Sistema operativo	**Mac O.S. 10.13**
	Impiego	**Servizi istituzionale (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Sala Cinema**
	Incaricato	**Fruitore del servizio**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook 13" (2008)**
	Sistema operativo	**Mac O.S. 10.6**
	Impiego	**Servizi istituzionali (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Sala Cinema**
	Incaricato	**Fruitore del servizio**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook 15" (2012)**
	Sistema operativo	**Mac O.S. 10.12**
	Impiego	**Servizi istituzionali (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Bari**
	Ufficio	**Servizio**
	Incaricato	**Antonella Liuzzi**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook 13" (2017)**
	Sistema operativo	**Mac O.S.**
	Impiego	**Servizi istituzionali (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Lecce**
	Ufficio	**Servizio/Cineporti**
	Incaricato	**Virginia Panzera**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC fisso**
	Modello	**MacMini (2010)**
	Sistema operativo	**Mac O.S. 10.6**
	Impiego	**Servizi istituzionali (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Lecce**
	Ufficio	**Servizio/Cineporti**
	Incaricato	**Luciano Schito**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook 12" (2012)**
	Sistema operativo	**Mac O.S. 10.11**
	Impiego	**Servizi istituzionali (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Lecce**
	Ufficio	**Servizio/Cineporti**
	Incaricato	**Antonio Serafino Gigante**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook 13" (2017)**
	Sistema operativo	**Mac O.S 10.13**
	Impiego	**Servizi istituzionali (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto Lecce**
	Ufficio	**Servizio/Cineporti/Proiezioni**
	Incaricato	**Sara Venturoli Galizia**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC**
	Modello	**Macbook**
	Sistema operativo	**Mac O.S.**
	Impiego	**Servizi istituzionali (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

SER	**Sede**	**Cineporto**
	Ufficio	**Servizio/Ufficio stampa**
	Incaricato	**Nicola Morisco**
	Amministratore sistema	**HSH Informatica & Cultura**
	Custode password	
	Descrizione	**PC portatile**
	Modello	**Macbook**
	Sistema operativo	**Mac O.S.**
	Impiego	**Servizi istituzionali (progetti)**

Disponibilità

X	*Stand alone*		*In rete non al pubblico*		*In rete pubblica*

Antivurus

	Con programma antivirus	X	*Senza antivirus*

E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti

La Titolare è dotata di appositi impianti di videosorveglianza composto in totale da 16 telecamere, quelle esterne registrano H24 le zone perimetrali esterne che non interessate dall'attività lavorativa necessarie per esigenze di tutela del patrimonio aziendale, quelle interne invece sono localizzate nelle aree di passaggio la cui presenza è sempre giustificata dalle medesime esigenze di cui sopra; a differenza di

quelle esterne, queste ultime entrano in funzione al termine dell'attività lavorativa dalle 20 alle 08.00 del giorno dopo.

I dati vengono custoditi temporaneamente e per non più di 24 ore all'interno del DVR, in una sala Server appositamente adibita ad accesso controllato da parte dell'Amministratore Delegato, per poi essere cancellati, salvo che non si rendano necessari alle Autorità di P.S. e P.G. per gli adempimenti di competenza.

Periodi di conservazione più lunghi sono previsti in caso di chiusura della sede e durante il week end per cui la registrazione parte dal venerdì sera ore 19.00 e termina il lunedì successivo ore 8.00, salvo casi in cui durante il week end non vi siano eventi; in tal caso le registrazioni vengono bloccate.

F – Altri strumenti

La Titolare è dotata di un proprio sito Internet http://www.apuliafilmcommission.it/

1.3 LA MAPPA DEI TRATTAMENTI EFFETTUATI

Le due principali coordinate sopra esposte nei paragrafi 1.1. e 1.2. (*natura dei dati* e *strumenti utilizzati*) costituiscono la base di partenza, per elaborare **l'elenco dei trattamenti** di dati personali, posto in essere dall'organizzazione: tale fase, che è in ogni caso necessaria per comprendere quali misure di sicurezza debbano essere adottate, deve formalizzarsi ***in un documento di gestione del rischio privacy secondo gli attuali approcci di "Privacy by design e by default***, da parte dei soggetti che sono tenuti a redigerlo. Operativamente, tale elenco può essere sintetizzato in una matrice, nella quale s'incrociano:

- **i tipi di dati personali che vengono trattati**; ed è, a tale riguardo, opportuno entrare in un grado di dettaglio maggiore, di quello offerto dalla semplice distinzione dati generici / particolari / giudiziari. Una particolare attenzione deve essere dedicata al *rischio per la privacy* insito nel trattamento, perciò una banca dati contenente informazioni di carattere genetico non può essere accomunata ad un'altra banca dati, anche se quest'ultima ha per oggetto dati particolari, ma di diversa natura.
- **gli strumenti che vengono utilizzati per il trattamento;** non ci si può limitare a distinguere gli strumenti elettronici, da quelli diversi, ma si deve entrare in un maggiore grado di dettaglio: in primo luogo, mantiene piena validità, nella sostanza, la circostanza che un elaboratore sia o no in rete, e se questa sia privata o pubblica, nonostante dal punto di vista delle misure minime da adottare la distinzione non abbia più rilevanza formale. Nell'ipotesi in cui il database aziendale, contenente dati particolari si trovi fisicamente su di in un computer in rete pubblica, questo aumenta tendenzialmente i rischi per la sicurezza, rispetto all'ipotesi in cui esso venga trattato con un elaboratore che non è in rete. Altro criterio distintivo, è quello che si basa sulla localizzazione degli strumenti: ad esempio, una rete di computer, dislocati in uffici ai quali si accede dopo avere varcato cinque porte blindate, offre maggiori garanzie di sicurezza di un'altra rete, avente caratteristiche tecniche analoghe, i cui terminali sono però dislocati in uffici poco protetti, nei quali vi è un notevole passaggio. Incrociando le coordinate di cui ai due paragrafi precedenti, si ottiene la mappa dei trattamenti di dati personali effettuati dal Titolare. In relazione al diverso grado di

rischio, è opportuno distinguere i trattamenti che vengono posti in essere nelle distinte aree in cui sono dislocati gli strumenti. Il simbolo X, significa che determinati tipi di dati sono trattati con determinati strumenti:

TIPI DI DATI TRATTATI		***STRUMENTI UTILIZZATI***																					
Cod.	***Descrizione***	***A1***	***A2***	***A3***	***A4***	***A5***	***A6***	***A7***	***A8***	***A9***	***B***	***C***	***D1***	***D2***	***D3***	***D4***	***D5***	***D4***	***D5***	***D6***	***D7***	***E1***	***E2***	***F***
Cod.01	*Dati contabili*	///	X	///	X	///	///	X	///	X			///	X	///	X	///	///	X	///	X	///	///	
Cod.02	*Dati interenti al personale dipendente*	X	X	///	///	///	///	///	///	X			X	X	///	///	///	///	///	///	X	///	///	
Cod.03A	*Dati relativi al servizio prestato: progetti e gestione progettazione*	///	X	X	X	X	X	X	///	X			///	X	X	X	X	X	X	///	X	///	///	
Cod 03B	*Dati relativi al servizio prestato: produzione e progetti audiovisivi*	///	X	///	X	X	X	X	///	X			///	X	///	X	X	X	X	///	X	///	///	
Cod 03C	*Dati relativi al servizio prestato: Film Found*	///	X	///	X	X	X	X	///	X			///	X	///	X	X	X	X	///	X	///	///	
Cod 03D	*Dati relativi al servizio prestato: Cineporti*	X	X	///	X	X	X	X	///	X			X	X	///	X	X	X	X	///	X	///	///	
Cod 03E	*Mediateca*	///	X	X	///	///	///	///	X	X			///	X	X	///	///	///	///	X	X	///	///	
Cod.04	*Altri tipi di dati comuni relativi ad altri soggetti relativi a contatti non sistematici.*	///	///	X	///	///	///	///	X	X			///	///	X	///	///	///	///	X	X	X	X	

Legenda degli strumenti utilizzati per il trattamento:

A – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:	**A1** - localizzati nella stanza adibita a sede della Direzione **A2** - localizzati nella stanza adibita a sede dell'Amministrazione **A3** - localizzati nella stanza adibita a sede della Segreteria **A4**- localizzati nelle stanze adibite a Progettazione e gestione progetti **A5**- localizzati nelle stanze adibite a Produzione e progetti audiovisivi **A6**- localizzati nelle stanze adibite a gestione Film Fund **A7**- localizzati nelle sedi e nelle stanze adibite alla gestione dei Cineporti **A8 -** presso Mediateca Regionale Bari **A9 –** Archivio ad accesso controllato
B – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:	//////////////////
C – Elaboratori in rete privata	//////////////////
D – Elaboratori in rete pubblica	**D1** - localizzati nella stanza adibita a sede della Direzione **D2** - localizzati nella stanza adibita a sede dell'Amministrazione **D3** - localizzati nella stanza adibita a sede della Segreteria **D4**- localizzati nelle stanze adibite a Progettazione e gestione progetti **D5**- localizzati nelle stanze adibite a Produzione e progetti audiovisivi **D6**- localizzati nelle stanze adibite a gestione Film Fund **D7**- localizzati nelle sedi e nelle stanze adibite alla gestione dei Cineporti **D8 -** presso Mediateca Regionale Bari
E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti	**E1 – Interno (Cineporto Bari)** **E2 - Perimetrale esterno (Cineporto Bari/FdL)**
F – Altri strumenti (es. basati su dati biometrici).	//////////////////

Da una prima lettura della mappa, si possono apprezzare gli accorgimenti adottati per ridurre i rischi:

- *in generale, i dati comuni vengono trattati ed archiviati da PC collegati anche in rete e, periodicamente consegnati in "forma controllata" a terzi, principalmente consulenti esterni, che li adoperano per trattamenti successivi finalizzati ad adempimenti civilistici, fiscali e amministrativi in forza di specifici obblighi di legge. I restanti dati sono conservati in azienda per il conseguimento degli scopi aziendali, o a P.A. e organi di controllo per le attività di "rendicontazione" di spesa e per particolari eventi gestiti dalla Titolare e che comportano l'utilizzo di fondi pubblici.*

2. *MANSIONARIO PRIVACY ED INTERVENTI FORMATIVI DEGLI INCARICATI*

Il trattamento dei dati personali viene effettuato da tutti i soggetti designati all'interno dell'organizzazione e che hanno ricevuto adeguata informativa, anche a mezzo accettazione dei regolamenti e delle procedure applicate in azienda.

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni e procedure in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- *corretto utilizzo della postazione di lavoro;*
- *corretto utilizzo degli apparati in dotazione;*
- *procedure da seguire in caso di assenza del lavoratore per l'accesso ai dati;*
- *procedure di gestione del dato cartaceo ed elettronico*
- *procedure di clean desk;*
- *procedure di gestione del back up*
- *procedure da seguire per la classificazione dei dati, al fine di distinguere quelli particolari e giudiziari (qualora dovessero ricorrere nel trattamento), per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune;*
- *modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti;*
- *modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave;*
- *prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;*
- *procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;*
- *procedure per il salvataggio dei dati;*
- *modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali;*

- *dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.*

Ai soggetti incaricati della gestione e manutenzione del sistema informativo (ditta esterna), siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

2.1 I RESPONSABILI DEL TRATTAMENTO

Nell'ambito della gestione dei trattamenti, il ***titolare ha l'obbligo ai sensi dell'art. 28 del vigente GDPR*** di nominare **uno o più responsabili**, anche mediante suddivisione dei compiti. I confini generali di tale ruolo vengono delineati dal combinato disposto degli articoli 28 del regolamento, La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare. In particolare, il soggetto identificato come responsabile deve:

• presentare garanzie sufficienti di attuare misure adeguate di protezione

• trattare i dati sulla base di un chiaro rapporto contrattuale (natura, finalità, durata del trattamento, tipi di dati, categorie di interessati, obblighi e diritti)

• trattare i dati solo sulla base di istruzioni documentate (non determina i mezzi)

• garantire l'impegno o il vincolo alla riservatezza degli incaricati

• mettere a disposizione tutte le informazioni per comprovare la conformità

• impegnarsi a cancellare i dati al termine della prestazione di servizi

Se un responsabile viola il regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento.

È bene specificare che il responsabile non si limita ad essere il mero esecutore delle istruzioni impartitegli dal titolare, poiché le caratteristiche di esperienza, capacità tecnica, affidabilità e conoscenza della legge, poste come condizioni necessarie per la sua nomina, lo qualificano come soggetto in grado di integrare, da un punto di vista pratico e tecnico, le scelte strategiche che il titolare, non necessariamente dotato delle capacità tecniche idonee, ha intrapreso in ordine al trattamento dei dati personali.

Il responsabile deve procedere al trattamento attenendosi alle istruzioni impartite dal

titolare che, anche attraverso verifiche periodiche, deve vigilare sulla puntuale osservazione delle disposizioni di legge e delle istruzioni impartite.

Il ruolo di responsabile può essere affidato a persone fisiche, persone giuridiche ed a qualsiasi altro ente, associazione od organismo, ***facenti o meno parte*** della organizzazione del titolare: quest'ultimo, se ritiene di farlo, può quindi nominare un proprio dipendente, un consulente esterno o una Fondazione terza.

La nomina deve avvenire ed essere accettata **per iscritto**, ed in essa si devono chiaramente specificare le istruzioni generali, impartite dal titolare, e descrivere analiticamente i compiti che al responsabile vengono da questi affidati. Indicativamente, in tale documento si devono individuare dettagliatamente:

- i dati personali e le banche dati di riferimento, oggetto di trattamento da parte del responsabile
- i trattamenti da svolgere, in funzione di ciascuna tipologia di dati personali, tenendo conto delle finalità del trattamento
- le misure di sicurezza da applicare
- i limiti di autonomia decisionale, nell'attività di gestione delle risorse (umane, tecniche, economiche), per effettuare il trattamento dei dati personali: a tale riguardo, è opportuno che al responsabile venga attribuita la possibilità di gestire in maniera autonoma un budget di spesa, dedicato agli adeguamenti richiesti per ottemperare alle disposizioni legislative e regolamentari
- i limiti di autonomia decisionale, in merito all'organizzazione tecnica ed umana per il trattamento dei dati personali
- i limiti di autonomia decisionale, in merito alle procedure di trattamento dei dati personali
- le responsabilità, che derivano dalle operazioni di trattamento: a tale riguardo, il responsabile risponde entro i limiti dei compiti e dell'esecuzione delle attività di trattamento di sua competenza, individuate dal titolare.

È opportuno che il conferimento della nomina di responsabile avvenga da parte di soggetto aziendale giuridicamente autorizzato che, nel caso di specie coincide con l'Amministratore delegato.

= = . = =

La Titolare, ai sensi dell'art. 4 del vigente Regolamento è la persona fisica, giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o congiuntamente, determina le finalità e i mezzi del trattamento.

La Fondazion e Apulia Film Commission è dotata di un'organizzazione impostata con criteri funzionali, si ritiene opportuno identificare nel Presidente del Presidente del C.d.A. la figura del Titolare del trattamento, in quanto può disporre le finalità e i mezzi del trattamento, nonché di designare quali Responsabili del Trattamento, figure apicali o comunque responsabili all'interno dell'Ente, e che sovraintendono particolari Uffici.

A tali figure si affiancano i Responsabili esterni appositamente nominati.

2.2 DATA PROTECTION OFFICER

In caso di nomina di questa particolare figura prevista dall'art. 39 del vigente Regolamento, chiamato nel testo in Italiano Responsabile della Protezione dei Dati (RPD), nominato obbligatoriamente da alcuni (e facoltativamente da tutti i titolari), il DPO si occupa di:

• considerare i rischi inerenti al trattamento

• informare e fornire consulenza al Titolare (e al responsabile) in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni relative alla protezione dei dati

• sorvegliare l'osservanza del Regolamento, delle altre disposizioni relative alla protezione dei dati e delle politiche del Titolare del trattamento

• fornire un parere in merito alla valutazione d'impatto e sorvegliarne lo svolgimento

• cooperare e fungere da punto di contatto con l'autorità di controllo

La sua funzione è in genere quella di *mantenere in efficienza* misure di sicurezza tali, da soddisfare le linee strategiche di indirizzo definite dal titolare. In tale ambito, i principali compiti possono essere, a titolo indicativo, i seguenti:

- di monitorare e suggerire i requisiti di sicurezza da adottare, per proteggere il complesso degli archivi, delle procedure e dei sistemi informatici esistenti: in particolare, dovranno essere definiti diversi livelli di requisiti funzionali, in relazione alla *valorizzazione* del patrimonio informativo da proteggere;

- di monitorare e suggerire un'architettura di sicurezza, che soddisfi i requisiti di cui sopra, con particolare riferimento alla armonizzazione delle misure di sicurezza con le architetture informatiche esistenti od in corso di implementazione;
- sovrintendere e sorvegliare il sistema di sicurezza, con particolare riferimento alla:
  - identificazione degli elementi da proteggere
  - identificazione delle minacce a cui detti elementi sono sottoposti
  - analisi dei rischi ed elaborazione della relativa *mappa*
  - analisi costi / benefici;
- pianificazione ed esecuzione di test del sistema di sicurezza, attraverso adeguate prove di penetrazione;
- definizione ed attuazione di piani e strumenti di monitoraggio continuo della sicurezza;
- aggiornamento periodico del sistema di sicurezza, per renderlo sempre adeguato alle nuove minacce;
- verifica della manutenzione del sistema di sicurezza, per assicurarne costante efficienza e disponibilità;
- supporto alla formazione del personale dell'organizzazione, in tema di sicurezza;
- emanazione di procedure interne inerenti la sicurezza (regolamentazione degli accessi fisici e logici agli archivi ed ai sistemi informativi, norme operative di utilizzo e gestione dei sistemi, gestione delle password, ecc).

Il compito di proporre, sviluppare e mantenere aggiornate le misure di sicurezza è di rilevante responsabilità e richiede alta professionalità e profonde conoscenze: per tale ragione, le organizzazioni meno strutturate possono decidere di avvalersi di un responsabile esterno, specializzato nella materia.

Per rivestire tale ruolo, proprio delle organizzazioni che trattano dati con l'uso di elaboratori elettronici, occorre infatti possedere un buon bagaglio di conoscenze tecniche nel campo dei sistemi informativi. Molte organizzazioni, con particolare riferimento a quelle di più limitate dimensioni, possono quindi trovare conveniente ricorrere a specialisti esterni, invece che a personale interno.

= = . = =

Nel caso in esame la Fondazione Apulia Film Commission è tenuta ai sensi e per gli effetti dell'art. 37 del vigente Regolamento UE 679/2016, di tale figura in quanto partecipata da soggetti pubblici ed ed ha provveduto alla nomina di un professionista esterno in persona del Dott. Riccardo Pierno, esperto qualificato e dotato dei requisiti richiesti dalla vigente normativa.

2.3 DIRITTI ESERCITABILI DAI SOGGETTI INTERESSATI

Il Capo III dall'art. 12 all'art. 20 contempla i diritti a disposizione dell'interessato al trattamento dei dati personali, che vengono detenuti da un determinato titolare: uno tale strumento è molto penetrante, poiché ogni individuo può, con uno sforzo minimo, riappropriarsi del controllo sui propri dati personali ed imporre una serie di adempimenti a chi li tratta.

L'utente potrà, in qualsiasi momento, esercitare i diritti di seguito indicati:

Accesso ai dati personali: ottenere la conferma o meno che si in corso un trattamento di dati che lo riguardano e l'accesso agli stessi ed alle informazioni:

• Finalità del trattamento
• Categorie di dati trattati
• Eventuali destinatari
• Eventuali trasferimenti ed eventuali adeguate garanzie
• Periodo di conservazione
• Diritti dell'interessato (tra cui revoca del consenso e diritto di reclamo)
• Eventuale esistenza di un processo decisionale automatizzato

Il titolare del trattamento fornisce una copia dei dati personali. Se la richiesta avviene mediante mezzi elettronici, e salvo indicazione diversa, le informazioni sono fornite in un formato elettronico di uso comune.

Richiesta di rettifica o cancellazione degli stessi o limitazione dei trattamenti che lo riguardano; per "limitazione" si intende il contrassegno dei dati conservati con l'obiettivo di limitarne il trattamento in futuro. L'interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. L'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche

fornendo una dichiarazione integrativa (tenuto conto delle finalità del trattamento) L'interessato ha diritto alla limitazione del trattamento, vale a dire di richiedere la sola conservazione, se:

• ha contestato l'esattezza dei dati (per il periodo necessario per verificare)

• il trattamento è illecito (ma ha richiesto la limitazione anziché l'oblio)

• i dati sono necessari all'interessato in sede giudiziaria, benché il titolare non ne abbia più bisogno

• ha esercitato il diritto di opposizione (mentre il titolare verifica l'esistenza di motivi legittimi e prevalenti)

Se è stata esercitata la limitazione, trattamenti ulteriori alla conservazione possono essere effettuati solo per: consenso dell'interessato, sede giudiziaria, tutela dei diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante.

Diritto all'oblio

L'interessato ha il diritto di ottenere la cancellazione dei dati che lo riguardano senza ingiustificato ritardo se:

• non sono più necessari rispetto alle finalità

• revoca il consenso (e non sussiste altro fondamento giuridico per il trattamento)

• si oppone al trattamento per motivi connessi alla sua situazione particolare (e non sussiste alcun motivo legittimo prevalente)

• si oppone al trattamento per finalità di marketing diretto

• i dati personali sono stati trattati illecitamente

• devono essere cancellati per adempiere un obbligo legale

• i dati personali appartengono ad un minore di 16 anni

Il titolare del trattamento è obbligato a cancellare i dati. Se li ha resi pubblici è obbligato ad informare gli altri titolari della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione degli stessi. Il diritto all'oblio non si applica se il trattamento è necessario:

• per l'esercizio del diritto alla libertà di espressione e di informazione

• per l'adempimento di un obbligo legale

• per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri

• per motivi di interesse pubblico nel settore della sanità

• a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

• per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Opposizione al trattamento: opporsi per motivi connessi alla Sua situazione particolare al trattamento di dati per l'esecuzione di un compito di interesse pubblico o per il perseguimento di un legittimo interesse del Titolare;

Portabilità dei dati: nel caso di trattamento automatizzato svolto sulla base del consenso o in esecuzione di un contratto, di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati che lo riguardano; in particolare, i dati Le verranno forniti dal Titolare in formato .xml, o analogo;

Revoca del consenso al trattamento per finalità di marketing, si diretto che indiretto, ricerche di mercato e profilazione; l'esercizio di tale diritto non pregiudica in alcun modo la liceità dei trattamenti svolti prima della revoca.

= = . = =

I predetti diritti potranno essere esercitati inviando apposita richiesta al Titolare del trattamento all'indirizzo privacy@apuliafilmcommission.it, gestito dal DPO.

La Fondazion Apulia Film Commission ha dato evidenza sul proprio sito di questa opportunità pubblicando apposite informative.

Qualora si riscontrino problematiche non risolvibili in maniera interna all'Ente, l'interessato ha diritto di proporre reclamo ai sensi dell'art. 77 GDPR all'autorità di controllo competente in base alla sua residenza abituale, al luogo di lavoro oppure al luogo di violazione dei suoi diritti; per l'Italia è competente il Garante per la protezione dei dati personali, contattabile tramite i dati di contatto riportati sul sito web www.garanteprivacy.it

Le richieste relative all'esercizio dei diritti dell'utente saranno evase senza ingiustificato ritardo e, in ogni modo, entro un mese dalla domanda; solo in casi di particolare complessità e del numero di richieste tale termine potrà essere prorogato di ulteriori 2 (due) mesi.

Il conferimento dei dati da parte dell'utente è obbligatorio in quanto necessario alla resa del servizio richiesto; pertanto, l'eventuale rifiuto da parte dell'utente, di fornire i

dati può comportare la mancata prestazione de servizio, nella misura in cui tali dati siano necessari a tali fini.

Il Regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 101/2018 (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Per i **dati "particolari"** (si veda art. 9 regolamento) il consenso **DEVE** essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

NON deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati particolari);

inoltre, il titolare (art. 7.1) **DEVE** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Il consenso dei minori è valido a partire dai 16 anni (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

DEVE essere, in tutti i casi, libero, specifico, informato e inequivocabile e NON è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).

DEVE essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.

= = . = =

La Fondazione Apulia Film Commission, in persona del suo DPO garantisce costantemente i predetti diritti, ed è particolarmente attenta alle esigenze degli

interessati, avendo predisposto adeguati sistemi per l'esercizio dei loro diritti attivando il canale mail privacy@apiliafilmcommission.it, o per il tramite della Segreteria.

2.4 *PREDISPOSIZIONE E AGGIORNAMENTO DEL SISTEMA DI GESTIONE DELLA PRIVACY*

Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa (***mansionario privacy***), nell'ambito del trattamento dei dati personali.

Con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

Nella seguente matrice si riassumono i tratti salienti dell'attuale mansionario privacy, come segue:

- sull'asse verticale si riportano i dati personali oggetto di trattamento, quali emergono dall'analisi effettuata nel paragrafo 1. del presente documento;
- sull'asse orizzontale si riportano le unità organizzative in cui si suddivide l'organizzazione del Titolare;
- l'apposizione del simbolo **X**, in corrispondenza della casella di intersezione tra le due coordinate, significa che una determinata unità organizzativa procede al trattamento dei dati indicati nelle righe:

TIPI DI DATI TRATTATI		*UNITÁ ORGANIZZATIVE*										
Cod.	*Descrizione*	*A1*	*B1*	*B2*	*C1*	*C2*	*D*	*E*	*F1*	*F2*	*F3*	*G*
Cod.01	*Dati contabili*	X	X	///	X	///	///	///	///	///	///	///
Cod.02	*Dati interenti al personale dipendente*	X	X	X	///	///	///	///	///	///	///	///
Cod.03	*Dati relativi al servizio prestato*	X	X	X	X	X	X	X	X	X	X	X
Cod.04	*Dati relativi a trattamenti non sistematici*	X	X	///	X	X	X	X	X	X	X	X

La legenda delle unità organizzative è la seguente:

Direzione	Area Amministrazione E Personale	Area Progettazione e Gestione progetti	Area Prod. e programmazioni audiovisive	Film Found	Cineporti	Mediateca
A1 Direzione	B1 - Amministrazione B2 – Personale B3 - Finanziario	C1 – RUP C2- Progettazione	D – Produzione	E – Film Found	F1 - Bari F2 - Lecce F3 - Foggia	G - Mediateca

2.5 *PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI E DEL PERSONALE PREPOSTO*

Gli **interventi formativi degli incaricati del trattamento** devono essere programmati in modo tale, che essi abbiano luogo *almeno* al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione dell'introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti rispetto al trattamento di dati personali.

Gli interventi formativi, che possono avvenire all'interno e/o presso soggetti esterni specializzati, devono essere finalizzati a rendere gli incaricati edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;

modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

Sono previsti interventi formativi degli incaricati del trattamento, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

La sensibilizzazione alle tematiche della sicurezza, ed a costanti comportamenti coerenti con le disposizioni date in merito, deve interessare tutte le risorse umane dell'organizzazione, ad ogni livello di responsabilità ed attività: ciò al fine di diffondere una cultura generalizzata della sicurezza, che consenta tra l'altro di favorire la miglior efficacia ed efficienza delle misure prese, oltre che di sopperire ad eventuali mancanze delle stesse.

L'azienda deve tenere presente che le attività relative alla sicurezza non rappresentano un appesantimento del lavoro quotidiano, ma una volta che entrano nel ciclo standard delle operazioni da compiere, contribuiscono a garantire il personale dal rischio di perdere, o comunque compromettere, parte del lavoro fatto.

A titolo d'esempio, presentazioni, opuscoli, seminari, riunioni dei dirigenti con i propri collaboratori possono rappresentare opportunità per raggiungere quest'obiettivo.

Per la corresponsabilizzazione, si deve prevedere di:

- coinvolgere i dirigenti e le rappresentanze degli addetti, in tutte le fasi di definizione del piano per la sicurezza;
- effettuare interventi di richiamo, e se necessario adottare gli adeguati provvedimenti disciplinari, in caso d'inadempienze e/o superficialità in tema di sicurezza.

Analoghi processi devono essere previsti con eventuali partner e per i collaboratori esterni, privati e pubblici, persone fisiche e giuridiche, che interagiscono in modo significativo con l'organizzazione.

L'introduzione di un sistema di sicurezza, come di qualunque altro elemento che modifichi le modalità lavorative all'interno di una qualsiasi realtà, ha sicuramente un forte impatto sull'organizzazione. La formazione interviene in due momenti ben precisi del processo d'introduzione di un sistema di sicurezza:

- sensibilizzazione sulle problematiche della sicurezza e sulla loro importanza;
- conoscenza delle misure di sicurezza da adottare, e da gestire ai diversi livelli di responsabilità.

= = . = =

La Titolare a tale fine, provvederà a programmare due tipi di corsi, distinti secondo i destinatari:

- *il primo, indirizzato alle figure apicali e ai responsabili del trattamento, che dovrà prevedere cenni sulla normativa, indicazioni sulle politiche di sicurezza, analisi dei rischi;*
- *l'altro, indirizzato al personale operativo, che dovrà fornire indicazioni precise sui comportamenti da adottare, sia nelle operazioni quotidiane sia nelle situazioni d'emergenza.*

Questo perché, la formazione, se ben orientata, progettata e realizzata, può essere lo strumento più efficace per realizzare la diffusione delle politiche, degli obiettivi e dei piani dell'organizzazione in tema di sicurezza, in modo da minimizzare quella componente, sempre presente, che consiste nella resistenza al cambiamento.

Tali interventi formativi sono programmati in modo tale, da avere luogo al verificarsi di una delle seguenti circostanze:

- *già al momento dell'ingresso in servizio*
- *in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali*
- *in occasione dell'introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.*

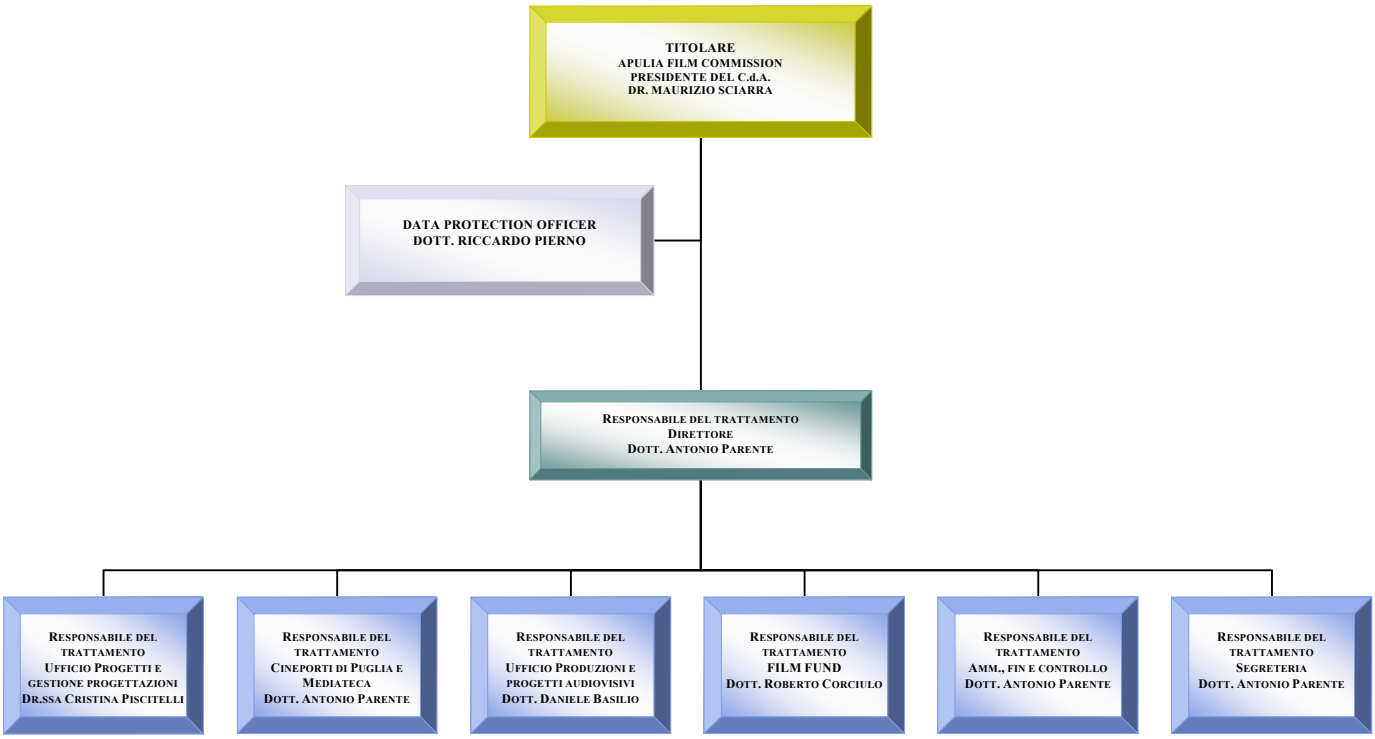
Tale Piano di formazione sarà automaticamente rivisto in sede di aggiornamento del presente documento, e comunque in relazione alle mutate esigenze dell'organizzazione ed allo sviluppo delle tecnologie.

Gli interventi formativi potranno avvenire sia all'interno, a cura del responsabile per la sicurezza o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.

2.5.1. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Descrizione intervento formativo	*Personale Interessato*	*Tempi previsti*
Introduzione al regolamento Europeo 679/2016	*Tutte le aree*	*Entro il 2018*
Analisi sistema privacy e procedure	*Tutte le aree*	*Entro il 2018*

2.6 ORGANIGRAMMA NOMINATIVO "PRIVACY"



3. *ANALISI DEI RISCHI CHE INCOMBONO SUI DATI*

Per quanto concerne i **tipi di dati**, essi possono in talune ipotesi costituire la ***fonte primaria di rischio***: si pensi ad esempio al database della clientela, il cui trafugamento è passibile di arrecare nocumento non solo all'organizzazione che lo possiede, ma anche ai clienti, ai quali i dati si riferiscono.

In funzione dell'*appetibilità* dei dati trattati, nonché dell'*idoneità* degli stessi ad arrecare danno ai soggetti interessati, i vari tipi di dati si considereranno portatori di un diverso grado di rischio, che potrà essere evidenziato in termini numerici o in termini qualitativi (es. rischio *elevatissimo* per i dati genetici, *modesto* per i dati comuni scaricati da Internet). 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.

Si precisa che l'analisi svolta non tiene conto solo del rischio intrinseco legato alla perdita o uso improprio del dato personale, ma anche alla più ampia analisi dedicata a tutti i dati gestiti dall'azienda, la cui perdita e/o uso improprio, potrebbe esporre l'organizzazione a problemi e danni anche maggiori. Nella seguente tabella si evidenziano i fattori di rischio cui sono soggetti gli strumenti con cui l'organizzazione procede al trattamento dei dati personali. Il simbolo 🗝*, posto nella casella di intersezione, significa che l'esposizione al rischio è minima; il simbolo* 🔥 *significa*

che l'esposizione al rischio è moderata, il simbolo 🔑 *significa che l'esposizione al rischio è elevata.*

TIPI DI DATI TRATTATI							STRUMENTI UTILIZZATI														
	A1	A2	A3	A4	A5	A6	A7	A8	A9	B	C	D1	D2	D3	D4	D5	D6	D7	D8	E1	E2
Rischio d'area, legato al verificarsi di eventi distruttivi	🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔥			🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔑
Rischio d'area, legato all'accesso non autorizzato nei locali	🔥	🔥	🔥	🔥	🔥	🔥	🔥	🔥	🔥			🔥	🔥	🔥	🔥	🔥	🔥	🔥	🔥	🔥	🔥
Rischio di guasti tecnici di hardware, software e supporti	////	////	////	////	////	////	////	////	////			🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔑
Rischio di penetrazione logica nelle reti di comunicazione	////	////	////	////	////	////	////	////	////			🔥	🔥	🔥	🔥	🔥	🔥	🔥	🔥	🔑	🔑
Rischio legato ad atti di sabotaggio e ad errori umani	🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔑			🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔑	🔥	🔥

Legenda degli strumenti utilizzati per il trattamento:

A – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:	**A1** - localizzati nella stanza adibita a sede della Direzione **A2** - localizzati nella stanza adibita a sede dell'Amministrazione **A3** - localizzati nella stanza adibita a sede della Segreteria **A4**- localizzati nelle stanze adibite a Progettazione e gestione progetti **A5**- localizzati nelle stanze adibite a Produzione e progetti audiovisivi **A6**- localizzati nelle stanze adibite a gestione Film Fund **A7**- localizzati nelle sedi e nelle stanze adibite alla gestione dei Cineporti **A8 -** presso Mediateca Regionale Bari **A9 –** Archivio ad accesso controllato
B – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:	//////////////////
C – Elaboratori in rete privata	//////////////////
D – Elaboratori in rete pubblica	**D1** - localizzati nella stanza adibita a sede della Direzione **D2** - localizzati nella stanza adibita a sede dell'Amministrazione **D3** - localizzati nella stanza adibita a sede della Segreteria **D4**- localizzati nelle stanze adibite a Progettazione e gestione progetti **D5**- localizzati nelle stanze adibite a Produzione e progetti audiovisivi **D6**- localizzati nelle stanze adibite a gestione Film Fund **D7**- localizzati nelle sedi e nelle stanze adibite alla gestione dei Cineporti **D8 -** presso Mediateca Regionale Bari
E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti	**E1 – Interno (Cineporto Bari)** **E2 - Perimetrale esterno (Cineporto Bari/FdL)**
F – Altri strumenti (es. basati su dati biometrici).	//////////////////

N.B.

Nell'elaborare la tabella, si è tenuto conto anche di alcuni fattori legati alla struttura del Titolare, nei seguenti termini:

- il rischio d'area, legato all'eventualità che persone non autorizzate possano accedere nei locali in cui si svolge il trattamento, è giudicato inferiore per l'area ad accesso controllato, all'interno della palazzina, rispetto a quanto accade per gli altri luoghi in cui si svolge l'attività, con conseguente diminuzione del rischio:
  - per gli archivi esistenti in tale area
  - per gli elaboratori in rete privata, in relazione al fatto che i server sono ubicati in tale area
  - per i personal computer non in rete, localizzati in tale area
  - il rischio di guasti tecnici delle apparecchiature interessa i soli strumenti elettronici: in tale contesto, è giudicata più rischiosa la situazione degli strumenti non in rete che, essendo affidati a singoli che non sempre possiedono un bagaglio tecnico adeguato, presentano un rischio di rottura maggiore, rispetto agli impianti che vengono gestiti da persone con specifiche competenze, quali quelli in rete, quello di sorveglianza e quello per la rilevazione di dati biometrici
  - il rischio di penetrazione logica nelle reti di comunicazione interessa, essenzialmente, i soli strumenti che sono tra loro collegati tramite una rete di comunicazione accessibile al pubblico
  - il rischio legato ad atti di sabotaggio, o ad errori umani delle persone, presente in tutte le tipologie di strumenti utilizzati, è maggiore per quelli che sono in rete.

Di seguito si commentano brevemente i rischi più frequenti, cui sono sottoposte alcune delle principali categorie di strumenti:

Risorse Hardware: rientrano in questa categoria CPU, terminali, workstation, personal computer, stampanti, disk drive, linee di comunicazione, server, router. Le principali minacce cui questi dispositivi sono sottoposti sono legate ai mal funzionamenti, dovuti a guasti o sabotaggi, eventi naturali quali allagamenti e incendi, furti e intercettazione. Quest'ultima minaccia interessa gli apparati di rete, cioè le linee di comunicazione, i router ed i server: è, infatti, possibile effettuare il monitoraggio indebito, o l'alterazione della trasmissione di dati, effettuata da questi apparati, sia che questa avvenga tra terminali, tra computer, tra stazioni di lavoro periferiche e sistemi centrali di elaborazione. Un altro caso può riguardare i video, intercettando le onde elettromagnetiche emesse dai quali si può procedere alla ricostruzione remota dell'immagine.

Risorse Software: rientrano in questa categoria Sistemi Operativi e Software di Base (utility, diagnostici), Software Applicativi, Gestori di basi di dati, Software di rete, i programmi in formato sorgente e oggetto, ecc. Le minacce principali legate all'uso di questi prodotti sono sono:

- la presenza di errori involontari, commessi in fase di progettazione e/o implementazione, che consentono ad utenti non autorizzati l'esecuzione di operazioni e programmi riservati a particolari categorie di utenti
- la presenza di un codice malizioso, inserito volontariamente dai programmatori dell'applicazione stessa, al fine di poter svolgere operazioni non autorizzate sul sistema, o per danneggiare lo stesso. Rientrano in questa categoria di minacce i virus, i trojan horse, le bombe logiche, le backdoor

- attacchi di tipo *denial of service*, che vengono generalmente portati a servizi di rete, ma sono facilmente estendibili a un qualunque servizio. Si tratta di attacchi non distruttivi, il cui obiettivo è saturare la capacità di risposta di un servizio, con il fine ultimo di renderlo inutilizzabile agli altri utenti del sistema.

Documentazioni Cartacee: le principali minacce a cui tali elementi sono sottoposti sono la distruzione e/o l'alterazione ad opera di eventi naturali, di azioni accidentali e di comportamenti intenzionali.

Supporti di memorizzazione: si tratta dei supporti su cui vengono tenute le copie dei software installati, dei file di log, dei back-up e dei dati personali. Oltre alle minacce cui sono sottoposte le documentazioni cartacee, tali dispositivi sono soggetti a:

- deterioramento nel tempo
- inaffidabilità del mezzo fisico, che in alcuni casi può presentare difetti di costruzione che ne compromettono il buon funzionamento nel tempo.

È evidente che esiste una *relazione inversa* tra il grado di rischio, cui sono sottoposti gli strumenti, e l'insieme delle misure atte a proteggerli, che vengono adottate: a tale riguardo, si fa presente che, se l'analisi dei rischi è finalizzata a adottare nuove e più efficaci misure di sicurezza, al termine di tale processo il grado di rischio, che grava su alcuni o su tutti gli strumenti impiegati, è destinato ad abbassarsi. In questi casi è opportuno che, in sede di analisi dei rischi, si proceda ad una duplice valutazione del grado di rischio che grava sugli strumenti, procedendo a stimarlo:

- sia nello *stato iniziale*, prima cioè che vengano adottate le nuove misure di sicurezza
- che nello *stato finale*, allorché le nuove misure previste saranno operative.

= = . = =

Nel caso in esame, le strutture fisiche di protezione delle aree e dei locali in cui si effettua il trattamento sono idonee poiché separate, anche se spesso condivise con altri soggetti quali utenti occasionali, per effetto dei servizi istituzionali prestati dalla Titolare e, per tale motivo il rischio legato all'accesso non autorizzato resta moderato.

Per via dell'attività svolta dalla Titolare il fattore di rischio legato ad eventi naturali e non, di ordine distruttivo ed a penetrazione di terzi, può considerarsi basso.

La Titolare risulta dotata di misure di sicurezza logica avanzate a livello centralizzato, e si ritiene di dover associare un fattore di rischio moderato, che tiene conto del rischio derivante da furto o perdita precoce dei dati non passati nel server per le attività di back up.

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità

per soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono;

- quelli legati alle caratteristiche degli strumenti utilizzati per procedere al trattamento dei dati.

Si tiene a precisare che la Titolare ha eseguito una stima del rischio e misure di protezione non solo incentrate su quanto richiesto dal GDPR in materia di protezione dei dati personali, ma anche con specifico riferimento ai "dati aziendali" la cui perdita, furto e/o uso improprio (si pensi ai cliché dei marchi gestiti), potrebbe causare gravissimi danni ai terzi e alle aziende titolari di quei marchi, con conseguente esposizione della Titolare ad azioni risarcitorie di importi rilevanti.

Per tali motivi particolare rilevanza in termini di apprezzamento del rischio è stato dato al dati relativi alla procedura identificati al codice 03

Per la Titolare sono stati attribuiti i seguenti coefficiente di rischio (range 1-7):

TIPOLOGIA DI DATI / GRADO DIINTERESSE PER I TERZI	***CODICI***	***RISCHIO (MEDIA)***
Dati relativi alla Contabilità	***Cod. 01***	***2+1=1,5***
Dati relativi al personale dipendente	***Cod. 02***	***4+4=4***
Dati relativi all'attività svolta	***Cod. 03***	***4+4=4***
Altri dati gestiti in forma residuale e non altrimenti classificabili	***Cod. 04***	***1+2=1,5***

Si riportano i giudizi, sul grado di rischio nello stato iniziale, nell'esempio oggetto d'analisi (range 1-7):

	TIPOLOGIA DI SUPPORTI / PERICOLO PRIVACY INTERESSATO	***RISCHIO (MEDIA)***
A	*schedari ed altri supporti cartacei*	***3+3=3***
B	*elaboratori in rete privata*	***-***
C	*elaboratori in rete con altri, e dotati di accesso ad Internet (rete pubblica)*	***2+4=3***
D	*Videosorveglianza*	***1+2=1,5***
E	*altri strumenti (sito Internet))*	***1+1=2***

RISULTATI MATRICE DI RISCHIO	***CODICI***	***STRUMENTI***	***APPREZZAMENTO DEL RISCHIO***
Dati relativi alla Contabilità	***Cod. 01***	***A+C***	***BASSO***
Dati relativi al personale dipendente	***Cod. 02***	***A+C***	***BASSO***

Dati relativi all'attività svolta	***Cod. 03***	***A+C***	***MODERATO***
Altri dati gestiti in forma residuale e non altrimenti classificabili	***Cod. 04***	***A+C+D+E***	***BASSO***

Si stima il grado di rischio, che dipende dalla ***tipologia dei dati trattati dal Titolare e dagli strumenti impiegati per il trattamento****, 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	TIPI DI DATI TRATTATI								
		ELEVATO							
		ALTO							
		MEDIO							
					COD. 03	COD. 02			
		BASSO							
				COD. 04	COD. 01				
			BASSO			MEDIO		ALTO	ELEVATO
			PERICOLOSITÁ PER LA PRIVACY DELL'INTERESSATO						
			STRUMENTI IMPIEGATI PER IL TRATTAMENTO						

N.B.

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 sensibile o giudiziario dei soggetti interessati, 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, commerciale e tecnologica, per il Titolare, in relazione ai danni che conseguirebbero da un'eventuale perdita, o trafugamento, dei dati.

4. *MISURE ATTE A GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI*

Nel presente paragrafo vengono descritte le procedure atte a garantire:

- la protezione delle aree e dei locali, nei quali 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 dell'utilizzo degli strumenti elettronici.

Si procede alla descrizione:

- delle procedure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento;
- delle ulteriori misure, finalizzate ad incrementare la sicurezza nel trattamento dei dati, la cui adozione è stata programmata, anche per adeguarsi alle novità introdotte dal GDPR;

4.1 *LA PROTEZIONE DI AREE E LOCALI*

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, *gli edifici ed i locali nei quali si svolge il trattamento sono in linea con la più recente normativa in materia di sicurezza e protezione dei luoghi di lavoro, conformemente a quanto previsto dal D.Lgs 81/08 e successive modifiche e integrazioni. protetti da:*

- *dispositivi antincendio;*
- *gruppo di continuità dell'alimentazione elettrica;*
- *cartellonistica di sicurezza;*
- *impianto di condizionamento;*
- *Piani di emergenza e di evacuazione.*

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da:

- *sistemi di allarme e di sorveglianza antintrusione;*
- *vigilanza diurna da parte del personale aziendale appositamente istruito e notturna da parte del personale interno durante il lavoro notturno e ditta esterna*

appositamente incaricata.

Gli impianti ed i sistemi di cui è dotata l'organizzazione:

- *appaiono soddisfacenti, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti. Per l'anno 2018 non sono previsti interventi di manutenzione e/o aggiornamento salvo l'immediato intervento in caso di guasti e riparazioni.*

4.2 LA CUSTODIA E L'ARCHIVIAZIONE DI ATTI, DOCUMENTI E SUPPORTI

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, dischetti, fotografie, pellicole), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti (vds Procedura Regolamento sull'utilizzo delle postazioni di lavoro e dei dispositivi aziendali e di *Clean Desk*)

4.2.1. AFFIDAMENTO AGLI INCARICATI E LA CUSTODIA DI ATTI E DOCUMENTI

Agli incaricati vengono date disposizioni di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, hanno l'obbligo di rivolgersi al responsabile di funzione, o ad un responsabile del trattamento, o direttamente al titolare.

Di conseguenza, gli incaricati devono prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli/riporli all'archivio, al termine di tale utilizzo.

4.2.2. ARCHIVIAZIONE DI ATTI E DOCUMENTI

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati particolari e giudiziari ove esistenti: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale, che ai dati non possano

accedere persone prive di autorizzazione. A tale fine, gli incaricati lavorano in un contesto dove la titolare ha messo loro a disposizione:

- *cassetti con serratura;*
- *armadi chiudibili a chiave;*
- *cassaforte;*
- *locali muniti di porta con serratura;*

nel rispetto delle procedure e dei regolamenti in essere, gli incaricati devono riporre i documenti, contenti dati, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi.

Al termine del trattamento, l'incaricato dovrà invece restituire all'archivio gli atti, i documenti ed i supporti non più necessari per lo svolgimento delle proprie mansioni lavorative.

Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni aziendali.

Particolari cautele sono previste per l'archiviazione di documenti, atti e supporti contenenti dati giudiziari: essa deve avvenire in luoghi, armadi, casseforti, o dispositivi equipollenti, che possono essere chiusi.

Gli archivi normalmente non contengono dati particolari o giudiziari e sono comunque controllati, mediante l'adozione dei seguenti accorgimenti:

- *i dipendenti tutti, e in particolare coloro che hanno le scrivanie prospicienti l'archivio, hanno il dovere di vigilare sugli accessi, controllando chi vi accede e, soprattutto, se è autorizzato dal Titolare o dal Responsabile del Trattamento;*
- *a tutti i dipendenti è stata fornita l'istruzione operativa di chiudere a chiave la propria stanza per impedire l'accesso non vigilato a quegli archivi custoditi all'interno della stessa, atteso che non tutte le scaffalature sono dotate di serrature;*

Al fine di tutelare la privacy degli interessati, e di limitare al minimo l'eventualità che gli stessi siano asportati, manomessi, o utilizzati impropriamente, non è in alcun modo

consentito al personale dipendenti e/o a terzi l'accesso agli archivi fuori dagli orari lavorativi. Gli stessi vengono opportunamente chiusi, e solo in casi del tutto eccezionali potrà essere loro consentito l'accesso, previa autorizzazione da parte del Titolare.

Gli impianti e le attrezzature, di cui è dotato l'Ente per la custodia e l'archiviazione di atti, documenti e supporti, appaiono soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti. Per l'anno 2018, sono quindi previsti semplicemente interventi di manutenzione e di rimpiazzo ove necessario con dotazioni più sicure.

4.3 LE MISURE LOGICHE DI SICUREZZA

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

- *realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato;*
- *realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative;*
- *realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus);*
- *prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (floppy disk, dischi ZIP, CD….), nei quali siano contenuti dati personali.*

4.4 ADOZIONE DI UN 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 solo per gli strumenti elettronici che, ove esistenti, 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 segue i principi di *privacy by default e by design*, che non solo permette di verificare l'identità della persona (accesso file log per) ma che ha predefinito il livello di accesso alle informazioni sul server per ogni utente.

Per realizzare le credenziali di autenticazione è stata utilizzata la seguente metodologia:

- *si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema internamente (Titolare), ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, comunque sbloccabile dal Titolare ricorrendone determinati presupposti, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente almeno ogni sei mesi.*

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri riportati qui sinteticamente e meglio dettagliati nella Privacy Password Policy attuata dall'azienda:

- *ad ogni incaricato le credenziali vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale;*
- *nei casi in cui una componente della credenziale di autenticazione è costituita dal codice per l'identificazione (username), attribuito all'incaricato da chi amministra il sistema, tale codice deve essere univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi;*
- *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;*
- *in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.*

Sino ad allora, limitatamente agli elaboratori che non sono in rete (ove esistenti), saranno presenti alcuni casi in cui le credenziali di autenticazione non verranno disattivate, qualora ciò non fosse di fatto possibile (ad esempio, perché la medesima credenziale è stata attribuita a due o più incaricati, alcuni dei quali mantengono la qualità per accedere all'elaboratore).

Agli ***incaricati vengono impartite precise istruzioni*** *(vds regolamento per l'uso delle postazioni di lavoro e dei dispositivi aziendali**)** 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 (viene prescritto l'obbligo di utilizzare cassetti con serratura), che in quella in cui l'incaricato provveda a portare il dispositivo con sé (viene prescritto l'obbligo di custodirlo come se fosse una carta di credito). In ipotesi di smarrimento, l'incaricato deve provvedere immediatamente a segnalare la circostanza 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), attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:*
  - *immediatamente, non appena viene consegnata loro da chi amministra il*

sistema

- *successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.*

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, né consistere in nomi noti, anche di fantasia;*
- *buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.*

Fermo restando che è stata fortemente richiamata l'attenzione di ciascun incaricato sulla circostanza che la postazione lavorativa e le sue dotazioni non possono in alcun modo essere utilizzate per uso c.d. promiscuo ma solo per l'attività lavorativa prestata in favore della Titolare, con specifico riferimento alle password, è stato prescritto che la stessa 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 continuità operativa e di sicurezza del sistema, potrebbe però rendersi necessario accedere agli strumenti ed ai dati.

A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi possano alternativamente e, a seconda della procedura attivata dalla Titolare:

- *nominare un soggetto fiduciario che garantisca l'accesso alla posta elettronica in sua assenza attraverso specifica procedura;*
- *deposito della la parola chiave su un foglio di carta da inserire in una busta chiusa e sigillata;*
- *consegna della 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 suo 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.

4.5 ADOZIONE DI UN SISTEMA DI AUTORIZZAZIONE

Per quanto concerne le **tipologie di dati ai quali gli incaricati possono accedere**, ed i trattamenti che possono effettuare si osserva, come già detto, che è stato impostato un sistema di autorizzazione a livelli, al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare in relazione alle mansioni lavorative svolte da ciascuno di essi. Al di fuori di questi casi, le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e, se designato, dal responsabile, ovvero da soggetti da questi appositamente incaricati.

Il profilo di autorizzazione non viene in genere studiato per ogni singolo incaricato, ma è generalmente impostato per classi omogenee di incaricati (ad esempio, attribuendo un profilo di autorizzazione predefinito a seconda dell'area di appartenenza amministrazione e personale, commerciale acquisti e vendite, produzione e grafica ecc.). 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.

*Per quanto riguarda la **protezione, di strumenti e dati**, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.*

Il primo aspetto 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).

A tale fine, si è dotati di idonei strumenti elettronici e programmi che vengono aggiornati con cadenza periodica e che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno sottoporre ad aggiornamento in modalità automatica "auto-protect", almeno con cadenza ristretta.

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, è stata loro distribuita una procedura nella quale si elencano i comportamenti da tenere, e quelli da evitare.

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.

La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall.

Il terzo aspetto riguarda l'utilizzo di appositi programmi, la cui funzione è di prevenire la vulnerabilità degli strumenti elettronici, tramite la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete, e di correggere di conseguenza i difetti insiti negli strumenti stessi.

L'organizzazione si è da tempo dotata di tali programmi, per la protezione da malfunzionamenti degli strumenti elettronici, che provvede ad aggiornare con cadenza almeno annuale, che diventerà semestrale per quegli strumenti che dovessero iniziare a trattare dati sensibili o giudiziari

Per quanto concerne i **supporti rimovibili** (es. floppy disk, dischi ZIP, CD….), 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.*

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici:

- *appaiono nel loro complesso idonee al fine di garantire la necessaria sicurezza ai dati personali trattati. Per l'anno 2018, sono quindi previsti semplicemente interventi finalizzati all'aggiornamento, alla manutenzione ed a qualche rimpiazzo di componenti hardware e software.*

5. *CRITERI E MODALITÀ DI RIPRISTINO DEI DATI*

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, così come previsto dall'art. 32 del vigente GDPR, la Titolare che aveva già da tempo impostato rigide procedure sul punto ha, sulla base dell'audit svolto per la redazione del sistema di protezione privacy, preso atto di dover migliorare in base al proprio contesto specifico del contesto le proprie procedure di back up, ovvero tutte le misure tecniche e organizzative attivabili, per garantire un livello di sicurezza adeguato al rischio, che comprendono:

la cifratura dei dati personali;

la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

Il responsabile del trattamento dei dati deve assicurarsi di avere delle procedure di cifratura dei dati e la capacità di ripristinare l'accesso agli stessi in caso di attacchi hacker o guasti tecnici. In parole povere, questo significa avere delle procedure di backup dei dati sempre attive, e che consentano inoltre di cifrare il contenuto del backup stesso, in modo tale da renderlo inaccessibile a chi non conosca le necessarie password. Infine, il backup deve essere rapidamente ripristinabile.

Il programma di back up deve consentire di cifrare i file e i backup di database, server di posta o macchine virtuali, possibilmente consentendo che la cifratura dei dati avvenga lato client, ovvero prima che il backup compresso venga trasferito ad esempio verso destinazioni *offsite*.

Backup di database e server di posta.

Rilevazione automatica di possibili corruzioni di file da parte di virus *ransomware.*

Per rendere ancora più sicura l'integrità dei backup, l'esistenza di una opzione avanzata che consente di interrompere le procedure di salvataggio dei dati in caso di rilevazione di possibili file corrotti/criptati da virus *ransomware* (come Cryptolocker, Wannacry, ecc…). In questo modo, si evita che i backup possano essere a loro volta corrotti, mentre una notifica via email può essere inviata all'utente per renderlo subito consapevole del problema.

Pianificazione di backup automatici anche di natura incrementale, con l'attivazione di

notifiche di avvenuta esecuzione.

Per i dati trattati con strumenti elettronici, sono previste procedure di back up, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni (CD, dischi ZIP…..).

= = . = =

Il salvataggio dei dati trattati avviene come segue:

- *la frequenza è giornaliera in cloud o su server nel rispetto delle modalità e dei principi su nominati per i dati contabili;*
- *per tutti gli altri dati il back up è settimanale.*

6. *L'AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO*

Nei casi in cui il trattamento di dati personali o una parte del processo in questione venga affidato, in conformità a quanto previsto dal GDPR all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle previste dal Regolamento. Per la generalità dei casi, in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno della struttura del Titolare, sono impartite istruzioni per iscritto al terzo destinatario, che viene designato quale Responsabile del Trattamento di rispettare quanto prescritto per il trattamento dei dati personali sia esso soggetto italiano, comunitario o extra comunitario.

Qualora il trasferimento avvenga verso soggetti residenti in Paesi extra-Ue, la Titolare si impegna a verificarne per quanto possibile e, compatibilmente con la propria realtà operativa, il grado di organizzazione e la capacità di rispettare le istruzioni forniteli.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati **particolari o giudiziari**, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.

NB

Nell'ipotesi in cui il trattamento, di dati particolari o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano (scegliere uno dei seguenti punti):

- rilasci la dichiarazione di avere adottato idonee procedure così come previsto dal vigente GDPR;
- di conoscere eventuali loro soggetti esterni coinvolti nel trattamento e le opportune garanzie su questi soggetti.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta.

= = . = =

Nel caso in esame la Titolare si avvale di una serie di professionisti esterni ai quali vengono consegnati in forma controllata una serie di dati anche relativi a soggetti privati, questo al fine di eseguire specifici adempimenti inerenti al funzionamento dell'azienda. A titolo meramente esemplificativo, ma non esaustivo: paghe, contabilità, bilanci, adempimenti fiscali, □avori stico-previdenziali e contratti, gestione sito internet e apparecchiature di sicurezza.

Tutti i professionisti in questione sono stati designati Responsabili del Trattamento per i processi di propria competenza.

6.1 TRATTAMENTI AFFIDATI ALL'ESTERNO

Descrizione sintetica dell'attività esternalizzata	Trattamento di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Parte del processo di contabilizzazione della Titolare e adempimenti civilistici e fiscali	Cod.01/02/04	De Vito Ernesto – OdV Pierno Ruggiero – Amm, Fisco e Bil. Plantone Vito – Contabilità HSH Srl – Gestione informatica Pierno Riccardo – DPO Sigma Sistemi Srl	Designazione Lettera di impegno Deontologia professionale
Carteggio relativo al personale	Cod.02/04	De Vito Ernesto – OdV Stefanelli Nicola – RSPP Cafagna Eugenio – Medico competente Plantone Vito – Contabilità Pierno Fabrizio – Consulenza Lavoro Pierno Riccardo – DPO HSH Srl – Gestione informatica Temporary Spa – Gestione rapporti lavoro interinale	Designazione Lettera di impegno Deontologia professionale
Carteggio relativo a questioni di interesse legale relativi alla Titolare	Cod.01/02/03/04	Palumbo Giuseppe – Legale civile Garofalo Domenico – Legale civile Patroni Griffi Ugo – Legale civile Cartolano Roberto – Legale ammin.vo Persichella Sabino – Legale ammin.vo	Designazione Lettera di impegno Deontologia professionale
Carteggio relativo a questioni relativo al servizio prestato	Cod.03/04	De Vito Ernesto – OdV Pierno Ruggiero – Amm, Fisco e Bil. Plantone Vito – Contabilità HSH Srl – Gestione informatica Pierno Riccardo – DPO Palumbo Giuseppe – Legale civile Garofalo Domenico – Legale civile Patroni Griffi Ugo – Legale civile Cartolano Roberto – Legale ammin.vo Persichella Sabino – Legale ammin.vo	Designazione Lettera di impegno Deontologia professionale
Servizi di Pulizia affidati all'esterno	Cod. 01/02/03/04	Pulisan	Designazione

7. *CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA "DATA BREACH E PROCEDURE DI CONTINUITÀ OPERATIVA"*

I dati di un sistema sono sottoposti ad una serie di rischi, che ne minacciano continuamente la disponibilità, che possono andare dai mal funzionamenti hardware agli atti di vandalismo, perpetrati da intrusi informatici. È possibile ridurre al minimo gli effetti, spesso disastrosi, di tali eventi, predisponendo una serie di accorgimenti tecnologici, quali ad esempio:

- *Sistemi RAID (Redundant array of unexpensive disks)*: si tratta di hard disk multipli, visti però dal sistema operativo come un singolo disco. La principale proprietà di questi dispositivi è di garantire la disponibilità e l'integrità dei dati, anche nel caso di guasto hardware di uno dei dischi che compongono il sistema;
- *Back-up*: si tratta di una serie di procedure attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni. In caso di guasto hardware dei dischi è quindi possibile *ripristinare* il sistema nello stesso stato in cui si trovava, nel momento dell'ultimo back-up;

  I back-up dovrebbero essere automatizzati e a periodicità molto ristretta, e la gestione dei supporti dovrebbe scongiurare i disastri derivanti da cause fisiche (incendi, allagamenti): è importante quindi predisporre armadi ad isolamento termico e/o magnetico, nonché copie multiple dei back-up (si consideri che anche i dispositivi di back-up possono guastarsi), da tenersi in luoghi differenti e distanti tra loro;

Tuttavia, ritenendo l'argomento Back up esaurito nel paragrafo precedente, si forniscono maggiori dettagli Piano di continuità operativa, che costituisce la forma più sofisticata di protezione dai rischi.

Innanzitutto il GDPR agli artt. 33 e 34 contempla un nuovo istituto denominato "*Data Breach*" che riguarda una sostanziale violazione di sicurezza che ha comportato 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 (vd art. 4 p.12 e art. 54 del GDPR); secondo il GDPR, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e,

ove possibile, entro 72 ore, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato.

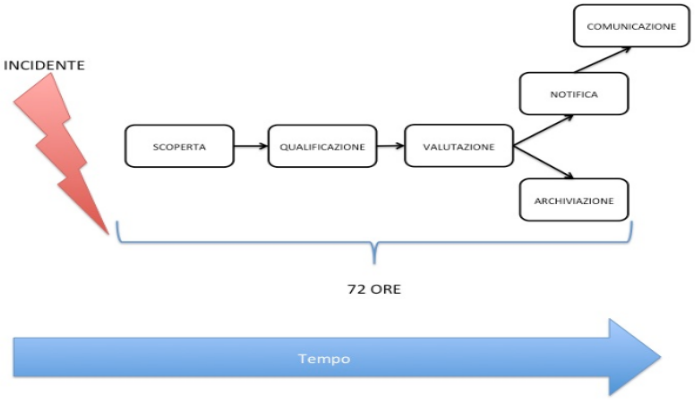
L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato, entro settantadue ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR, la imposizione di sanzioni amministrative.

= = . = =

Preliminarmente, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

A tale proposito, il Titolare del trattamento è stato istruito in merito alla identificazione dell'incidente di sicurezza e, dopo aver determinato l'impatto sulle informazioni e sulla specifica violazione, di valutare autonomamente la necessità, o meno, di procedere alla notifica diretta del data breach all'autorità di controllo (DPO), competente a norma dell'art. 55 GDPR e ss., o direttamente al Garante della Privacy seguendo l'iter logico di cui al presente schema



Il Titolare ha informato tutte le figure apicali (Responsabili del trattamento) nonché gli incaricati di procedere alle necessarie segnalazioni anche in presenza di semplici sentori che concernono presunte violazioni anche di dati non personali), in modo da poter aprire con tempestività la fase investigativa; le violazioni sono state distinte in tre macro categorie anche concorrenti tra loro:

1) violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.

2) Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;

3) Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Nel momento in cui il Titolare ha preso atto che la violazione abbia rappresentato una violazione delle liberta individuali, dispone la comunicazione all'interessato con l'ausilio dei format di legge previsti.

Il Piano di Continuità Operativa

Il piano di continuità operativa che determina la capacità di un sistema di essere resiliente, ha lo scopo di garantire la continuità e la disponibilità degli strumenti e dei dati, in ipotesi di danneggiamenti causati da eventi accidentali, sabotaggi, disastri naturali, furti. L'obiettivo del Piano di Continuità Operativa è di ripristinare i servizi informatici e operativi in genere dalla Titolare entro un tempo prestabilito, in funzione dei livelli di servizio attesi, e di rendere minime le perdite causate dall'interruzione dell'attività.

Ciò significa che il Piano di Continuità Operativa non deve essere inteso come misura

alternativa, a quelle di prevenzione, ma è un completamento di queste ultime, al fine di:

- garantire la continuità dei principali processi, assicurando l'erogazione dei servizi essenziali;
- limitare gli impatti degli eventi a carattere distruttivo sulla posizione finanziaria.

Il Piano di Continuità Operativa si occupa del controllo delle interruzioni di operatività, al fine di prevenirne e minimizzarne l'impatto, individuando un insieme specifico di contromisure di sicurezza, in grado di sostenere le operazioni critiche dell'organizzazione, anche attraverso infrastrutture alternative.

Lo scopo è di raggiungere e mantenere un sistema di operazioni che prevenga i rischi e, in caso di accadimento dell'evento distruttivo, ne limiti l'impatto sulla continuità dell'operatività: a tale fine, sarebbe opportuno attivare un processo di sviluppo e mantenimento di specifici piani, che includano misure di identificazione e riduzione del rischio orientate a limitare le conseguenze di un impatto dannoso, e ad assicurare un rapido ripristino delle operazioni essenziali.

Il processo di pianificazione della Continuità Operativa dovrebbe essere visto come un quadro di riferimento per la gestione di più procedure di ripristino, orientate a coprire scenari di impatto differenziati, in relazione ai diversi eventi dannosi: dalla semplice caduta di alimentazione fino agli eventi catastrofici che richiedono un vero e proprio Piano di *disaster recovery* (con esso si intende l'insieme di soluzioni volte a ripristinare i sistemi informatici e fisici in caso di loro indisponibilità prolungata).

La Continuità Operativa è un processo continuo che si articola in attività di analisi, progetto, attuazione e manutenzione di un piano che deve contemplare:

- identificazione e classificazione per priorità di ripristino di processi ed operazioni critici;
- determinazione dei potenziali impatti di indisponibilità, rispetto ai diversi scenari di danneggiamento;
- identificazione delle responsabilità ed adozione di contromisure tecniche ed organizzative;
- documentazione dei processi e delle procedure concordate (di emergenza, di continuità, di ripristino);
- formazione specifica di tutto il personale sui processi e le procedure della

Continuità Operativa;

- test, manutenzione ed aggiornamento del piano.

La realizzazione del Piano di Continuità Operativa si basa quindi su contromisure, di carattere sia tecnologico che organizzativo, che indicano cosa fare, con quali risorse, e quali procedure seguire in condizioni di emergenza, che rendano il sistema informativo parzialmente o totalmente indisponibile.

I principali *aspetti tecnologici* riguardano:

- il recupero dei supporti di back-up;
- il recupero delle transazioni perse;
- il Disaster Recovery, nel caso di impatto per evento catastrofico. In questo caso la principale contromisura di carattere tecnologico consiste nel centro di back-up, che può essere realizzato in uno dei seguenti modi:
  - predisponendo una struttura tipo *scatola vuota*, di proprietà dell'organizzazione, o di tipo consortile o in service;
  - raddoppiando il centro ed integrandolo in rete;
  - creando un centro di recovery che può essere di proprietà dell'organizzazione, o di tipo consortile o in service.

Dovrà inoltre essere predisposta una struttura di commutazione, che in caso di emergenza sia in grado di commutare l'utenza dal sistema principale a quello di back-up.

I principali *aspetti organizzativi* riguardano la definizione del piano dettagliato di chi fa cosa, dal momento della dichiarazione dello stato di emergenza a tutto il periodo (anche diversi mesi) durante il quale il centro primario potrebbe rimanere fuori servizio. Nulla deve essere lasciato al caso, per cui il piano dovrà comprendere:

- l'assegnazione delle responsabilità individuali;
- le procedure di rilevamento e segnalazione;
- il Piano di gestione dell'emergenza;
- l'organizzazione della ripartenza delle operazioni essenziali (ripartenza automatica);
- il Piano di gestione della comunicazione verso le Direzioni, altre organizzazioni, il pubblico;

- corsi di sensibilizzazione e formazione periodici;
- la manutenzione del Piano: organizzazione di test regolari e revisioni di tutte le contromisure, le procedure ed i recovery plan.

L'*attività di manutenzione* del piano riveste particolare importanza, per evitare che il sistema stesso divenga rapidamente obsoleto ed inefficace a causa della:

- evoluzione tecnologica dei sistemi hardware e software, sia del proprio sistema informativo che, eventualmente, di quello del Centro di Back-up;
- evoluzione organizzativa e logistica dell'organizzazione;
- cambiamento delle persone che occupano i ruoli interessati. Se il piano non segue tempestivamente questi cambiamenti, perde di efficacia in breve tempo; l'unico modo per verificare che la manutenzione sia effettuata in modo adeguato è quello di programmare prove reali, o almeno "di carico", almeno due volte all'anno.

Si precisa che, nell'ambito delle misure minime di sicurezza, non è in generale previsto l'obbligo di adottare un piano di continuità operativa (salvi casi particolari, in cui la perdita di dati sarebbe di particolare nocumento per le persone cui essi si riferiscono), la cui complessità lo rende per inciso accessibile solo alle organizzazioni di rilevanti dimensioni: anche per esse, in considerazione del fatto che i Piani di Continuità in genere richiedono investimenti significativi, per la loro realizzazione, e' importante che essi vengano definiti, tenendo continuamente presente un corretto rapporto costi/benefici, nei limiti della loro effettiva necessità.

= = . = =

La Titolare ha il compito di aggiornare le procedure di sicurezza, al fine di adottare gli strumenti e le conoscenze rese disponibili dal progresso tecnico e tecnologico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle procedure di sicurezza adottate, la Titolare con il supporto dei responsabili di funzione provvede, ad effettuare una verifica sulle seguenti attività:

- *verificare l'accesso fisico ai locali dove si svolge il trattamento;*
- *verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;*

- *monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite: attraverso quest'analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette;*
- *verificare l'integrità dei dati e delle loro copie di back up;*
- *verificare la sicurezza delle trasmissioni in rete;*
- *verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti;*
- *verificare il livello di formazione degli incaricati.*

Almeno una volta l'anno, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.

8. *VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI DPIA E REGISTRO DEI TRATTAMENTI*

La valutazione d'impatto sulla protezione dei dati (DPIA, acronimo di "Data Protection Impact Assessment") è un processo che il titolare del trattamento deve effettuare quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35 GDPR).

La DPIA dovrebbe stabilire chi ha la responsabilità delle singole misure finalizzate alla gestione dei rischi e alla tutela dei diritti e delle libertà degli interessati e può anche essere utile per valutare l'impatto di protezione di dati di un prodotto tecnologico, per esempio un componente hardware o software, qualora ciò sia suscettibile ad essere utilizzato da altri titolari per effettuare diversi trattamenti.

La DPIA è obbligatoria solo qualora un trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, paragrafo 1), come meglio chiarito dal paragrafo 3 dell'art. 35 e integrato da quanto prevede il paragrafo 4 dello stesso articolo, tra i quali:

a) trattamenti valutativi e di scoring, incluse la profilazione ed attività predittive: in particolare a partire da "aspetti concernenti le prestazioni della persona interessata al lavoro, la situazione economica, la salute, le preferenze o interessi personali, l'affidabilità o il comportamento, la posizione o gli spostamenti";
b) decisioni automatizzate con effetti giuridici o similmente significativi: si pensi a trattamenti finalizzati ad assumere decisioni su soggetti interessati e che producano "effetti giuridici riguardanti la persona fisica" o che "allo stesso modo siano determinanti per la persona fisica";
c) monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "la sorveglianza sistematica di un'area accessibile al pubblico" (art. 35, paragrafo 3, lettera c);
d) dati particolari o strettamente personali: si tratta delle categorie particolari di dati personali di cui all'art. 9 (per esempio, informazioni sulle opinioni politiche di una

persona fisica) oltre ai dati personali relativi a condanne penali o reati di cui all'art. 10;

e) i trattamenti di dati su larga scala: il Regolamento non definisce cosa costituisca larga scala, anche se il considerando 91 fornisce alcune indicazioni. In ogni caso, il WP29 raccomanda alcuni criteri di riferimento per determinare se il trattamento è effettuato su larga scala;

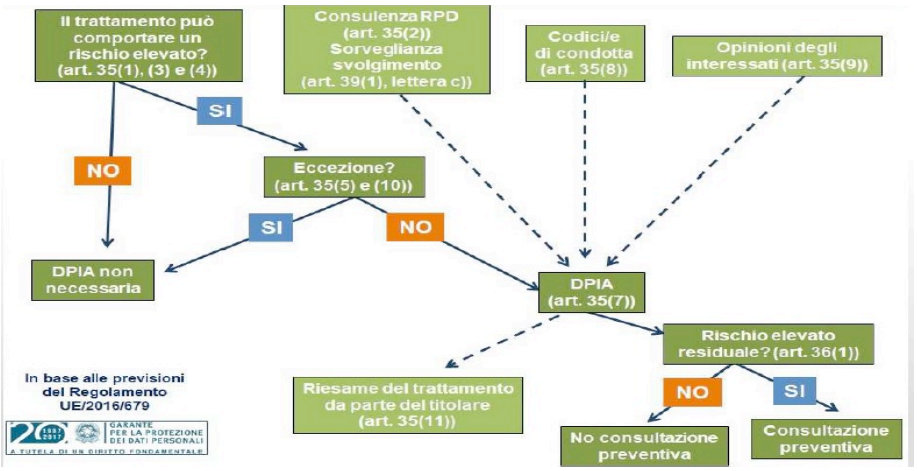
f) i dati relativi ad interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati può richiedere una DPIA a causa del maggiore squilibrio di potere tra l'interessato e il titolare, nel senso che il singolo può non disporre del potere di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti;

g) l'uso innovativo o l'applicazione di soluzioni tecnologiche o organizzative: ad esempio combinando l'uso di impronte digitali e il riconoscimento del volto per un migliore controllo degli accessi fisici, ecc.;

h) combinazione o raffronto di insiemi di dati: per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

i) tutti quei trattamenti che, di per sé, "impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (art. 22 e considerando 91): ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto. Si pensi, a titolo di esempio, allo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.

La DPIA viene svolta seguendo il seguente iter



Inoltre, il principio di responsabilizzazione prevede che ciascun titolare "tiene un registro delle attività di trattamento svolte sotto la propria responsabilità" comprendente, fra l'altro, le finalità del trattamento, una descrizione delle categorie di dati e i destinatari dei dati stessi, nonché "ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1" (art. 30, paragrafo 1) e deve valutare se vi sia la probabilità di un rischio elevato anche se potrà decidere, in ultima analisi, di non condurre una DPIA.

= = . = =

Attesi i dati trattati e le attività svolte, la Titolare pur conoscendo a tutti i livelli gli iter della DPIA ha inteso comunque non attivare il Registro dei Trattamenti previsto dalla normativa in quanto oggettivamente e soggettivamente non tenuta, avendo comunque provveduto nel presente documento ad identificare tutti i dati ritenuti utili anche ai fini della compilazione del registro per tutti i trattamenti opportunamente distinti per processi e, sugli stessi, identificati rischi e procedure di contenimento.

9. *DICHIARAZIONI D'IMPEGNO E FIRMA*

Il presente documento, redatto per la prima volta nel settembre 2018, viene emesso in data odierna in rev. 0, ed è da ritenersi un vademecum da utilizzare in quanto è inclusivo di una serie di istruzioni operative realmente adottate dall'organizzazione della Titolare secondo i principi di Privacy by design e by default.

In tutti i casi in cui è sorta l'esigenza di approfondire una serie di misure organizzative in materia di protezione dei dati personali, la Titolare ha predisposto una serie di Procedure indicate nelle revisioni del presente documento in sequenza numerica a partire dalla nr. 1 a seguire.

L'originale del presente documento viene custodito presso la sede della Fondazione, per essere esibito in caso di controlli, una sua copia verrà consegnata:

- *a ciascun responsabile del trattamento dei dati personali;*
- *a tutti gli incaricati anche mediante affissione nella bacheca dei lavoratori.*

Bari, lì 29 settembre 2018

_____

Il Titolare del trattamento
Il Presidente del Cda
Dott. Maurizio Sciarra

_____

Il Responsabile del Trattamento
Il Direttore
Dott. Antonio Parente

_____	_____	_____
Il Responsabile del Trattamento ***Uff. Progetti e Gestione Progettazioni*** ***Dr.ssa Cristina Piscitelli***	***Il Responsabile del Trattamento*** ***Cineporti di Puglia e Mediateca*** ***Dott. Antonio Parente***	***Il Responsabile del Trattamento*** ***Uff. Prod. e progetti audiovisivi*** ***Dott. Daniele Basilio***
_____	_____	_____
Il Responsabile del Trattamento ***Film Fund*** ***Dott. Roberto Corciulo***	***Il Responsabile del Trattamento*** ***Amministrazione, finanza e controllo*** ***Dott. Antonio Parente***	***Il Responsabile del Trattamento*** ***Segreteria*** ***Dr. Antonio Parente***

ALLEGATO A) – TABELLA DI SUPPORTO AL PARAGRAFO 1

PRIMA COORDINATA
TIPI DI DATI TRATTATI
(in neretto i dati trattati dalla titolare)

DATI SENSIBILI
DATI PARTICOLARI
Idonei a rivelare le origini razziali o etniche
- dati idonei a rivelare l'appartenenza ad un gruppo linguistico
Idonei a rivelare le convinzioni religiose; adesioni ad organizzazioni a carattere religioso
Idonei a rivelare le convinzioni filosofiche o di altro genere e le adesioni ad organizzazioni a carattere filosofico
Idonei a rivelare le opinioni politiche
Idonei a rivelare la adesione a partiti od organizzazioni a carattere politico
Idonei a rivelare la adesione a sindacati o organizzazioni a carattere sindacale
Idonei a rivelare lo stato di salute
- dati idonei a rivelare l'appartenenza a categorie protette
- dati idonei a rivelare l'identità del donatore
- dati idonei a rivelare l'identità del ricevente
- dati idonei a rivelare lo stato di disabilità
- dati idonei a rivelare sieropositività
- dati idonei a rivelare malattie infettive e diffusive
- dati idonei a rivelare malattie mentali
- dati relativi a indagini epidemiologiche
- dati relativi a prescrizioni farmaceutiche e cliniche
- dati relativi ad esiti diagnostici e programmi terapeutici
- dati relativi all'utilizzo di particolari ausili protesici
- dati relativi alla prenotazione di esami clinici e visite specialistiche
- dati idonei a rivelare AIDS conclamato
- dati inerenti a caratteristiche o idoneità psichiche
Idonei a rivelare la vita sessuale
- dati idonei a rivelare lo stato di gravidanza
DATI GENETICI
Dati idonei a rilevare patologie descritte nel registro nazionale delle malattie rare e/o in quelli regionali
Dati idonei a rilevare la gravità o il decorso del quadro clinico delle patologie genetiche
Dati idonei a identificare malattie ereditarie
Dati relativi alle malformazioni congenite la cui causa non è nota
Dati idonei ad accertare maternità o paternità
Dati relativi a indagini epidemiologiche
Dati relativi a indagini sulla popolazione
Dati relativi a trapianti di tessuti od organi o all'impiego di cellule staminali
Dati relativi alla procreazione
Dati tratti da studi di relazione tra patrimonio genetico e fattori di rischio

DATI BIOMETRICI
Caratteristiche della voce Geometria della mano Impronte digitali Informazioni di tipo comportamentale (andatura, movimento delle labbra, digitazione su tastiera...) Riconoscimento dell'iride o retina Rilevazione facciale attraverso uno o più elementi Combinazione di due o più elementi sopra indicati
DATI GIUDIZIARI
Dati relativi a comportamenti illeciti o fraudolenti Dati relativi a provvedimenti o procedimenti giudiziari Dati relativi a provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili
DATI DIVERSI DA QUELLI SENSIBILI E GIUDIZIARI
Nominativo, indirizzo o altri elementi di identificazione personale - **nome, cognome, età, sesso, luogo e data di nascita** - **indirizzo privato, indirizzo di lavoro, numero di telefono, di telefax o di posta elettronica** - **posizione rispetto agli obblighi militari** - **dati fisici (altezza, peso, ecc.)** - **dati idonei a rivelare l'origine nazionale** **Codice fiscale ed altri numeri di identificazione personale** - **carte sanitarie** - **numero carta di identità, passaporto, pat. di guida, numero di posizione previdenziale o assistenziale** - targa automobilistica **Dati relativi alla famiglia e a situazioni personali** - **stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare** **Istruzione e cultura** - **curriculum di studi e accademico** - pubblicazioni: articoli, monografie, relazioni, materiale audio-visivo, ecc. - **titoli di studio** **Lavoro** - **occupazione attuale e precedente** - **informazioni sul reclutamento, sul tirocinio o sulla formazione professionale** - **informazioni sulla sospensione o interruzione del rapp di lavoro o sul passaggio ad altra occupazione** - **curriculum vitae o lavorativo, competenze professionali** - **dati relativi alle pregresse esperienze professionali** - **retribuzioni, assegni, integrazioni salariali e trattenute, beni aziendali in possesso del dipendente** - **dati sulla gestione e sulla valutazione delle attività lavorative** - **cariche pubbliche rivestite**

- **dati relativi ad eventuali controversie con precedenti datori di lavoro**

Beni, proprietà, possessi

- **proprietà, possessi e locazioni; beni e servizi forniti o ottenuti**

Attività economiche, commerciali, finanziarie e assicurative

- **dati contabili, ordini, buoni di spedizione, fatture, articoli, prodotti, servizi, contratti, accordi, transazioni**
- identificativi finanziari, redditi, beni patrimoniali, investimenti
- **passività, solvibilità, prestiti, mutui, ipoteche**
- **crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi**
- **dati assicurativi, dati previdenziali**
- **dati relativi al comportamento debitorio**
- **dati relativi all'affidabilità o puntualità nei pagamenti**
- **dati relativi alla solvibilità economica**
- **dati relativi all'adempimento di obbligazioni**
- **dati relativi allo svolgimento di att. economiche e altre informaz. commerciali (es. fatturato, bilanci, aspetti economici, finanziari, organizzativi, produttivi, industriali, commerciali, imprenditoriali)**
- **dati relativi a comportamenti illeciti o fraudolenti**
- **dati relativi ad altri provvedimenti o procedimenti giudiziari**
- **dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, ammin. o contabili**

Dati su comportamento, abitudini di vita o di consumo

- creazione di profili di utenti, consumatori, contribuenti, ecc
- profili della personalità e dei tratti caratteriali
- viaggi, spostamenti, preferenze o esigenze alimentari (eccettuate quelle fondate su convinzioni religiose o filosofiche)
- dati sull'appartenenza ad associazioni diverse da quelle di carattere religioso, filosofico, politico o sindacale
- licenze, autorizzazioni (licenze di caccia o pesca, ecc.)
- dati relativi ad attività sportive o agonistiche
- dati idonei a rivelare scelte di consumo

Dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica

- dati idonei a rilevare immagini o suoni
- dati idonei a rilevare la posizione di beni, strumenti, oggetti
- dati idonei a rilevare la posizione di persone

SECONDA COORDINATA
CATEGORIE DI SOGGETTI CUI SI RIFERISCONO I DATI TRATTATI
(in neretto i dati trattati dalla titolare)

Abbonati
Addetti alla sicurezza
Aderenti ad associazioni politiche, religiose, sindacali o filosofiche
Agenti e rappresentanti
Agricoltori
Amministratori, coordinatori o altre persone che ricoprono incarichi in organismi di tipo associativo
Artigiani
Assistiti
Candidati a procedure concorsuali o selettive
Candidati da considerare per l'instaurazione di un rapporto di lavoro
Cittadini di Paesi appartenenti all'U.E.
Cittadini di Paesi non appartenenti all'U.E.
Cittadini italiani
Clienti o utenti (anche potenziali)
Commercianti
Concepiti e nascituri
Condannati, detenuti o sottoposti a misure di sicurezza o prevenzione
Coniugi e conviventi
Consulenti e liberi professionisti, anche in forma associata
Consumatori
Deceduti
Donatori o riceventi
Familiari dell'interessato
Fedeli
Fornitori
Genitori
Gruppi familiari
Gruppi omogenei per abitudini sessuali
Gruppi omogenei per altre caratteristiche
Gruppi omogenei per appartenenza razziale o etnica
Gruppi omogenei per area geografica
Gruppi omogenei per caratteristiche fisiche
Gruppi omogenei per consanguineità
Gruppi omogenei per fattori di rischio
Gruppi omogenei per nazionalità
Gruppi omogenei per provenienza geografica
Imprenditori individuali, piccoli imprenditori o liberi professionisti
Indagati o imputati
Lavoratori autonomi
Lavoratori o collaboratori
Maggiori di età

Malati gravi o sottoposti a particolari trattamenti di cura
Militari o appartenenti alle forze dell'ordine
Minori di età
Neonati (entro il primo anno di vita)
Parenti, affini o conviventi
Passeggeri su veicoli o utenti di mezzi di trasporto
Pazienti, degenti o disabili
Personale dipendente
Personale pubblico dirigenziale e magistrati
Persone affette
Persone fisiche
Persone giuridiche ed altri enti (comprende societa' di persone)
Persone in cerca di occupazione
Scolari o studenti di ogni ordine e grado
Soci o associati ad associazioni o fondazioni anche non riconosciute
Soci, associati, aderenti, iscritti e simpatizzanti (anche potenziali o non più facenti parte dell'organismo di tipo associativo)
Soggetti con limitata capacità di intendere e volere
Soggetti in difficoltà o pericolo (anche potenziali)
Soggetti o organismi pubblici
Utenti di servizi o impianti sportivi