

Appendix 1 to Cleriti DPA

1. Information on processing

The subject matter of the order processing is described in detail in the Subscription Agreement and the GTC. It essentially covers the following:

The Client stores information containing personal data on the portal provided by the Contractor (Cleriti) and shares reports containing personal data via the portal.

2. The nature and purpose of the processing are specified in the Subscription Agreement and include in particular:

The Client shall store on the Contractor's portal and send information via the Contractor's portal about the exploitation of audiovisual productions with associated personal data of authors and neighbouring rights holders.

3. The processing concerns the types of data listed below:

Possible personal data are usually name, profession/activity, address and e-mail address.

4. The following categories of data subjects are affected by the processing:

Authors and neighbouring rights holders who have contributed to audiovisual productions.

Appendix 2 to Cleriti DPA

General technical and organizational measures pursuant to Art. 32 GDPR

Technical and organizational measures			
<i>The Contractor shall design its internal organization in such a way that it meets the special requirements of data protection. In particular, measures shall be taken which, depending on the type of personal data or categories of data to be protected, are suitable to ensure an appropriate level of protection. The following measures are defined in detail:</i>			
No.	Measure	Implementation of the measure	
1	Physical access control <i>Note: Unauthorized persons must generally be denied access to data processing systems with which personal data is processed or used</i>	Yes	No
	Building security with alarm system	☒	☐
	Building surveillance by video, plant security or night watchman	☒	☐
	Measures to secure buildings with windows and shafts	☒	☐
	Automatic door locks (electric strikes and automatic door closers)	☒	☐
	Chip card/transponder locking system	☒	☐
	Manual locking system	☒	☐
	Defined access authorizations to the server room including key control and access logging	☒	☐
	Other:		

No.	Measure	Implementation of the measure	
2	Electronic access control <i>Note: Data processing systems must be prevented from being used by unauthorized persons.</i>	Yes	No
	Authentication with individual user name/password or biometric procedure	☒	☐
	Regulation of password allocation (type, duration, blocking)	☒	☐
	Assigning - access rights to users	☒	☐
	Automatic, password-protected computer lock	☒	☐
	Regulation for the deletion of authorizations of employees who have left the company	☒	☐
	Binding procedure for assigning authorizations	☒	☐
	Use of anti-virus software	☒	☐
	Encryption of data carriers	☒	☐
	Securing internal networks against unauthorized access from outside (firewall)	☒	☐
	Other:		

No.	Measure	Implementation of the measure	
3	Internal access control	Yes	No

	<i>Note: It must be ensured that those authorized to use a data processing system can only access the data subject to their access authorization. It must be ensured that personal data cannot be read, copied, changed or removed without authorization during processing, use and after storage.</i>		
	Creation of user profiles	☒	☐
	Create authorization concept with differentiated authorization levels	☒	☐
	Documentation of authorizations	☒	☐
	Regulation for copying data	☒	☐
	Deactivating or securing USB ports and burners	☒	☐
	Time limitation of access options (e.g. weekend)	☒	☐
	Other:		

No.	Measure	Implementation of the measure	
4	Data transfer control <i>Note: It must be ensured that personal data cannot be read, copied, changed or removed without authorization during electronic transmission or during transport or storage on data carriers.</i>	Yes	No
	Use of encryption in storage and transportation	☒	☐
	Access to personal data only via authenticated channels	☒	☐
	Documentation of the retrieval and transmission programs	☒	☐
	Evaluation options for the transmission logs	☒	☐
	Maintaining an overview of regular call-off and transmission processes	☒	☐
	Secure transport containers/packaging for physical transportation	☒	☐
	Use of e-mail encryption for personal data	☒	☐
	Data protection-compliant destruction of data carriers (e.g. misprints)	☒	☐
	Other:		

No.	Measure	Implementation of the measure	
5	Data entry control <i>Note: It must be ensured that it is subsequently possible to check and determine whether and by whom personal data has been entered, changed or removed from data processing systems.</i>	Yes	No
	Traceability of data entry, modification and deletion through individual user names (not user groups)	☒	☐
	Assignment of rights to enter, change and delete data on the basis of an authorization concept	☒	☐
	Deletion regulation for log data	☒	☐
	Other:		

No.	Measure	Implementation of	
-----	---------	-------------------	--

		the measure	
6	Order control <i>Note: It must be ensured that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.</i>	Yes	No
	Checking the data security precautions	☒	☐
	Appointment of a data protection officer	☒	☐
	Obligation of employees to maintain data confidentiality	☒	☐
	Ensuring the destruction of data after completion of the order (order is a.o. a subscription agreement)	☒	☐
	Other:		

No.	Measure	Implementation of the measure	
7	Availability control <i>Note: It must be ensured that personal data is protected against accidental destruction or loss.</i>	Yes	No
	Emergency concept in place for IT disruptions	☒	☐
	Redundant protection of servers and databases	☒	☐
	Uninterruptible power supply (UPS) in server rooms	☒	☐
	(Redundant) air conditioning in server rooms	☒	☐
	Automatic fire and smoke detection systems	☒	☐
	Fire extinguishing equipment in the server room	☒	☐
	Alarm messages for unauthorized access to server rooms	☒	☐
	Data backup and recovery concept	☒	☐
	Storage of data backups in a secure, off-site location	☒	☐
	Reconstruction of data sets and testing of data sets	☒	☐
	Use of virus scanners	☒	☐
	Automated updating of virus scanners	☒	☐
	Guidelines for the maintenance and implementation of updates	☒	☐
	Automatic and permanent monitoring to detect faults	☒	☐
	Other:		

No.	Measure	Implementation of the measure	
8	Isolation control <i>Note: It must be ensured that data collected for different purposes can be processed</i>	Yes	No

	<i>separately.</i>		
	Logical client separation	☒	☐
	Authorization concept with definition of access rights	☒	☐
	Separation of production and test system	☒	☐
	Other:		

Appendix 3:
Subcontractor according to clause 7.1

Name	Address	Service
Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521	Cloud Computing-Platform and services