Data Protection Impact Assessment (DPIA)

Identification of the need for a DPIA

The audiovisual material managed by our company is considered confidential and critical. The staff working in the production department as well as the collaborating actors and directors have direct contact with the audiovisual material we manage. No matter how strict the physical control is before entering the production area, there is always the risk of someone intentionally or unintentionally leaking some of the material. There are several ways that can occur, such as taking photo, copying a script, or some of the critical audiovisual material.

For all above reasons, there is a seriousness of any material leakage. Any issue of this kind will have serious financial damage and also legal consequences between our company and our customers. Surveillance by cameras, is a deterrent to someone committing such an act as it is also further evidence that someone has committed a malicious act.

Surveillance areas

The areas that the recording areas are placed are: the server room, the I/O data room, the controls of the recording post production studios and the mix post production studios.

Recording material management

Description of the nature of the processing:

The cameras recorder is placed into the server room. The recorded files are recorded on the internal hard drive of the machine and kept for 15 days. The machine automatically records on the old files so the history is always 15 days. These files are not circulated, they are not sent anywhere and they are checked only by Ciso and Ciso assistant in case of any incident.

Description of the processing:

The record files will be used in case of any incident, involving illegal activity concerning audiovisual material. All prohibited activities are described in the confidentiality agreement that all personnel entering on the production areas have accepted and signed. This process includes minors whose parents or guardians have signed a corresponding confidentiality agreement. In the confidentiality agreement there is an article that describes the existence of recording cameras in our premises that manage audiovisual materials. It is also described in which legal cases the recording material can be used. The staff that enters the monitoring areas are of all ages, from 7 years old as an actor and adults as sound engineers, technicians and directors.

Description of the purposes of the processing:

The reason for the recording as described above concerns the enhancement of the safety of the audiovisual materials. Physical security is not exhaustive so anyone that enter the production area carrying an image recorder is always possible. By monitoring the production areas we reduce the risk of using such devices that may pass into these areas secretly. The goal is to minimize the possibility of malicious action related to material leakage.

Assess necessity and proportionality

Description of compliance and proportionality measures:

The possibility for a company of recording and monitoring specific areas where critical - confidential material is distributed, is provided in the specific European and national legislation for personal data and in particular the General European Regulation 2016/679 and Laws 4624/2019 and 2472/1997. Especially article 27 par. 7 Law 4624/2019 which provides specifically for the registration in the workplace that:

The processing of personal data through closed-circuit visual recording within the workplace, whether publicly accessible or not, is permitted only if it is necessary to protect persons and property (for our company critical property is any audiovisual material). Data collected through closed-circuit optical recording may not be used as a criterion for evaluating employee efficiency. Employees are aware of the monitoring system by signing a non-disclosure agreement with our company.

Monitoring and recording the specific areas and the staff working in them, prevents any deliberate action that will cause damage to the company. Unfortunately, there is no other way to avoid any malicious action in these enclosed areas where there is no other visual control.

Data security ensurance:

Data security is ensured by the periodic inspection of ciso & ciso assistant

Criteria

1st Criteria Unit
Criteria for the systematic description of each of the processing operations under consideration.

1. Nature, scope, context and objectives are taken into processing.
2. The areas where audiovisual material is managed, are recorded. The recording material is kept on the hard disk of the recording machine, in the server room.
3. The processing of the recorded material, concerns cases of illegal activity occurs and concerns material leakage or intentional destruction of the audiovisual material/equipment. The recording material can be used in public court in order to prove that an illegal action is occurred.
4. There are no approved codes of conduct according to which our company should adjust the recording process. Our company acts according to the instructions of its customers who consider that their material should be protected from leakage or destruction.

2nd Criteria Unit
Criteria for assessing the necessity and proportionality of the treatment and the provisions of GDPR compliance measures

1. The measures to comply with the principles and legality of processing are analyzed in the section above “assess necessity and proportionality”.
2. The recording material is used appropriately, relevant and limited to what is absolutely necessary for the purposes of data processing
3. The retention time of the recording data is limited to 15 days.
4. The personal rights measures are insured to the highest data protection standards. A firewall has been installed in our facilities to reduce the risk of data interception through the closed recording circuit from any external factor. Also, the recording machine and files are kept in the safest room of the facility which is the server room. In the server room, only a limited number of people such as ciso, ciso assistant and the administration are allowed to access.
5. There is transparent information in the NDA signed by all employees and associates about the use of recording materials as well as the consequences in case of any

criminal act. In case of any change occur (of the terms of use of the right of the recording company / use of the recording materials of the employees and associates), a new NDA is being re-signing with the new terms.

6. Access and portability rights change only in the event of any change of administration or ciso and ciso assistant
7. There are no correction and deletion rights from any company member or associate in the recording materials.

3rd Criteria Unit

Criteria for the identification, analysis, assessment and management of risks for the rights and freedoms of employees and associates.

1. the origin, the nature, the probability (or the particularity) and the seriousness of the risks or equivalents for any risk of illegal access, authorized modification or loss of data have been evaluated.
2. The sources of risk have been taken into account by our company
3. The potential impact on the rights and freedoms of the employees and associates in cases of occurrence of the aforementioned risks have been assessed.
4. Risks of danger have been identified
5. The probability and severity of the risks have been assessed
6. The envisaged measures for dealing with the risks have been defined