Setkeeper is built to comply
with the highest security and data privacy
requirements

https://en.setkeeper.com/security/privacy/Email
contact@setkeeper.com
+1 818 530 4565

A Practical Guide to GDPR Compliance for Production Companies and Studios

It is necessary for all Production companies and Studios
to have data protection tools in place
to ensure compliance with the General Data Protection
Regulation provisions which come in effect
on May 25th 2018.

This Practical Guide is designed to help both your
productions and SetKeeper meet the new requirements
together.

SetKeeper

Are you are affected by GDPR?

As a Production Manager, am I affected by GDPR?

Yes. As a Line Producer, Production Manager, Production Coordinator, Casting Director, etc., you collect and are in control of data, so therefore you are bound by GDPR.

- You need to carefully define how you collect and regulate your data.
- You also need to have some defined key actions to comply with GDPR, such as having secured and encrypted systems in place, to protect the personal data you are managing.
- You need to have both processes, policies and softwares in place such as for example, Setkeeper.
- Also, keep in mind that an individual can be prosecuted for not complying to GDPR.

How can Setkeeper restrict data breaches?

- Implementing a secured and encrypted production platform such as Setkeeper can be very helpful in preventing data breaches.
- For example, our 2 factor authentication (2FA), PDF encryption, secured login vastly improve the secured handling and processing of personal data.
- When looking at technological solutions, we encourage you to choose the right software and technology to protect your data, to ensure it meets the highest security standard available.
- However, technology can only be as strong as your enforced privacy policies and processes: you therefore will be required to train and inform your crew about the need for strict GDPR compliance to regulate the distribution of personal data to align with your electronic web-based platforms.

1 Definitions and goals of GDPR

Definitions and goals

In order to cope with technological evolutions and the use of personal data, the GDPR consists to:

- Allow the citizens to have control over the use of their personal data;
- Create a uniform level of protection over the use of personal data in the UE;
- Define a legal framework adapted to the numeric evolution.

Personal data:
Any information related to a physical person identified or identifiable directly or indirectly, by reference to an identification number or to one or more elements to it.

Examples:

- Directly identifying personal data: name, surname, photography, videos, nominative emails, etc.;
- Indirectly identifying personal data: account identifier social security number employee number biometric data connection data localization data etc.;
- Gathering information.

WARNING:
Legal entities are not affected by the definition of personal data, which only covers individuals.

Thereupon, all data related to commercial partners (name, headquarters, RCS number, ie) should not be considered as personal data.

Data processing:
Any manipulation of data (automatized or not).

Examples:
Registration, consultation, remote access, organization, adaptation/ modification, broadcast, destruction, erasure, structuration, collection, archiving, transfer, etc.

Processing controller:
Physical or legal entity which determines the purpose of the treatment (reason for which the processing is realized) and the means of the treatment (measures implemented to obtain the purpose).

Examples of purposes:
Management of human resources, recruitment, access control to the premises, management of a client's database, commercial prospection.

Examples of means:
Computer hardware, informatics material, software, associated services, financial information, etc.

Processing processor:
Physical or legal entity which processes personal data on behalf of the controller

Main provisions

Some previous rights have been confirmed by the GDPR:

- The right to be informed;
- The right to access to one's personal data;
- The right of rectification;
- The right to oblivion;
- The right to object;
- The right to complain.

Rights created by the GDPR:

- Strengthening the information of the persons whose personal data are collected (right to complain DPO contact details right to erasure right to object);
- The right to erasure;
- The right to restrict the processing;
- The right to the portability of the processing (which permits to facilitate the transfer of personal data from a provider services to another, for example from a social network to another);
- Expansion of the case for the security breaches;
- The right to compensation;
- Specific conditions for children's personal data processing.

Sanctions

GDPR gives national control authorities the power to impose administrative penalties in case of violation of the rules of protection of personal data, according to a gradual system of financial penalties, depending on the severity of the offence.

For the administrative penalties, those can range from 10 to 20 million of euros depending on the category of offence.

For companies, the administrative penalties can be from 2% to 4% of the global annual sales of the previous financial year, whichever is the higher.

Other sanctions can include: law suit for compensation, injunction to comply, warning, publication of the sanction, damage resulting from tarnished reputation, etc.

In this context, it is necessary for Production companies to have data protection tools in place to ensure compliance with the regulatory provisions which come in effect on May 2018.

2 Personal Data Governance

Designate a DPO or data manager

According to the GDPR, you are required to designate a Data Protection Officer (DPO) if:

- you are a public authority or body;
- your core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale;
- your core activities consist of processing special categories of data as well as personal data on a large scale relating to criminal convictions and offences.

Even if the designation of a DPO is not compulsory in regard to your structure and the personal data processing, it is prudent to designate a data manager to be in charge of the personal data governance (information mission, advice and internal control procedures).

Manager's / DPO's functions

- Alerting the staff concerning issues of personal data protection.
- Manage and maintenance of the data register, software and database (updates, readability, etc.).
- Present annual report of processing activities.
- Mediation with the data protection authorities and the data subjects affected by the processing (clients, employees, etc.).

- Respect the Rights of Access, Modification, Opposition, portability, right to oblivion of people involved.
- Control the respect and application of legal regulation.

3 Create a Data Register

Principle

You are responsible for recording all data transactions carried out by your company.
The objective is 1/to anticipate the potential risks; 2/ to ensure a transparency of yourdata processing in case of compliance control.

Data register's form

A specific database form is not provided by the GDPR so you are free to create your own.
As a first step, we recommend creating a detailed excel table.

Register's content

- Mode of data collection (data collection form; contract etc.).
- Categories of the data subjects (clients, employees etc.).
- Proof of the data subject's consent and information of the data subjects concerning their rights.
- Different types of collected personal data (civil information, professional information, financial and economic information, location data, etc.).
- Reasons for individual data processing (customer relationship management, employment management, etc.).

- Identification of the person in charge of the processing (name, contact of the controller, its representative and the DPO or data driver) identification of the processor.
- Information related to the recipient, and where applicable, transfers to a third country or an international organization.
- Length of time before deletion of data.
- Description of the technical and organisational security standards.

Be aware that if you are processor, you also must create a register in order to list the controller, the categories of personal data collected for each controller, information about you (name, contact, representative, DPO etc.), information related to a transfer of the data to a third party/an international organisation and a description of the technical and organisational security measures.

4 Respecting The Rights of The Data Subjects

Rights of the data subjects

The data subjects (employees, clients, etc.) have specific rights (information, opposition, access, rectification, erasure, portability, etc.).
The right of erasure is to request to the controller the erasure of the data without undue delay when:

- **Personal data is not necessary anymore** regarding the purposes for which it was collected;
- **The data subject withdraw his/her consent or objects to the processing** of his/her personal data;
- Personal data that had been **unlawfully processed or for which there is no legitimate interest anymore**;
- Personal data should be erased following a legal obligation.

The right of portability is the right to acquire data contained within an existing format or received from a third party when:

- Personal data is "provided" by the data subject (date collection form for example);
- The automated processing is based on the consent of the data subject or on a contractual agreement executed with the data subject.

Following these steps will ensure you are in compliance with all individual rights for the processing of personal data.

For that, you should receive claims of the individuals concerned.

Communicate with the data subjects

Your company should establish data protection policy and internal procedures to ensure the processing and management of the data subject's requests.

To ensure this, it is recommended to:

- Determine the procedure applicable to the data subjects claims (dedicated email address; telephone number; regular mail, etc.) and inform the data subjects of this procedure;
- Verify the foundation concerning the data subject's request as regard to the existing conditions of their rights (erasure or portability for example).

Assign a person in charge of handling the request as well as communicating any delay or change in process.

5 Ensuring the Security of Personal Data and Inform in case of Infringement

Principle

As controller, you are liable of the security of personal data. Consequently, you must implement tools/work with qualified providers in order to ensure the security of the collected personal data.

In case of data security breach, you must notify the supervisory authority and the data subjects no later than 72 hours after becoming aware of it without undue delay.

Be aware that it is possible to hold both controller and processor positions. This is the case for example, when you are responsible for the categorization of collecting the data, its purpose, and storage duration (quality of controller), and at the same time have access to the client's database in order to manage it (quality of processor).

Controllers and processors should communicate to put into their contractual agreements some principal points:

- The processor should process personal data only according to the instructions given by the controller;
- The processor should ensure that employees adhere to confidentiality agreement;
- The processor should establish appropriate organizational and technical measures to ensure personal data is protected at a security level that is proportional to possible risks;
- The processor cannot subcontract the processing of the personal data without the prior written consent of the controller;
- Any contract between a processor and a processor from an inferior range should be under the same level of protection of personal data than those provided in the contract executed with the controller;
- The processor should assist the controller to ensure the adherence with the security obligations , the evaluation of the privacy impact assessment, in line with the guidelines of the supervisory authorities when processing data with a high risk level;
- The processor should delete or restore the personal data only after the processing is complete;
- The processor should provide the controller all necessary information to demonstrate conformity and compliance in the case of an audit.

Areas of responsibilities of the controller and the processor should be defined in writing. It has been indicated that an electronic format is considered valid. In this case, adjustments should be made to former contracts.

Procedure

- Application of effective solutions and software to ensure a level of security appropriate to the risk (pseudonymisation and encryption of personal data; safeguarding of continuous confidentiality, data integrity, availability and resilience of processing systems and services, etc.);
- Develop technical tools and processes to identify security vulnerabilities at all levels and/or have your technical service providers (processor) meet these requirements including the requirement of communicating any data security breach to you immediately;
- Implement technical measures to resolve any data security

breach and/or have your technical service providers (processor) implement such measures. Indeed, processors should establish organizational and technical measures to guarantee an appropriate level of security of personal data. They also should establish a policy of reporting violation in case of a violation of personal data;

- Prepare an email/letter to inform the supervisory authority which describes the nature of the personal data breach, the number and categories of data subject/records concerned, the name and contact details of the data protection officer, the likely consequences of the personal data breach, the measures taken to address the personal data breach;
- Prepare an email/letter to inform the data subject about the nature of the personal data breach, the measures taken to address the personal data breach, the name and contact details of the DPO;
- Ensure a traceability of the measures adopted to address the personal data breach.

6 Transparency of the Data Collection

Principle

Due to the liability principle imposed by the GDPR, you have to be able to prove that you have established process, policies and organizational measures to respect the GDPR.

Procedure

- Archive and centralize all information, documents, communications related to the collection of data (contracts/emails/documentation relative to the storage media and security for example).
- For any new data collection, adopt an impact assessment, record and store this analysis.
- Keep the proof of the clear and explicit consent of the data subjects (contracts signed; emails; data collection forms; etc.).
- Keep an accurate track record of the information of the data subjects concerned about their rights.
- Store the receipts and the processing records for the requests made by the data subjects concerned (erasure, rectification, portability, oblivion, etc.).