



**Privacy Laws and
Digital Media Libraries,
keeping you compliant**

SECTION 1/ PRIVACY LAWS AND TERMS IN BRIEF

INTRODUCTION

GDPR became EU law in May 2018, when the laws regarding the processing and storing of personal data became much stricter. Businesses had to decide which legal basis was most appropriate for them to use out of the six described which depended on the purpose and relationship with the individuals; consent, contract, legal obligation, vital interests, public task, legitimate interests, special category data and criminal offence data.

For marketers, consent or contract or legitimate interests represented the most appropriate basis for processing data, so privacy policies were revised accordingly, marketing lists cleaned and permissions and opt-ins acquired where necessary. The transition for many meant a substantial reduction in personal data and whatever that data was attached to – marketing lists, video, images and audio.

Today, ensuring personal data is processed in line with current legislation, which includes the PECR until it's replaced with the ePR in 2020, must be part and parcel of everyday practice in the workplace. Policies and procedures may have been replaced, but making sure consent continues to be acquired and stored correctly is another challenge.

Data terms:

The General Data Protection Regulation (GDPR)

GDPR, which came into force on 25 May 2018, aims to bring definition, clarity and accountability to data practice, and enforce transparency via a legal framework for a 'Single Digital Market'.

Data Protection ACT (DPA)

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It sits alongside the GDPR, and tailors how the GDPR applies in the UK - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

The Privacy and Electronic Communications (PECR)

The PECR regulation gives people specific privacy rights in relation to electronic communications. The EU is in the process of replacing the current e-privacy law with a new ePrivacy Regulation (ePR), estimated to be ready mid 2020. The existing PECR rules continue to apply until the new ePR is finalised, although when GDPR came into force, it amended the definition of consent within the PECR.

Source of terms: www.iso.org

SECTION 2/ DIGITAL MEDIA LIBRARIES: ENABLING COMPLIANCE

GUIDING PRINCIPLES OF GDPR

The GDPR means that all businesses dealing with personal data must implement the necessary technical and organisational changes in order to comply with the data protection principles set out by the ICO. One of most important principles that informs the daily working practices, processes and tools that businesses use is ‘data protection by design and by default’. Many digital media library applications have built-in tools to ensure data protection and security.

They offer features that will help with GDPR regulations, including the core principle of accountability. The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles. With digital media libraries users can track who has accessed what and where it’s been used, so that they can produce accurate audit trails and reports which enable you to demonstrate your compliance.

Another key principle of the GDPR is that you must process personal data securely by means of ‘appropriate technical and organisational measures’ – this is the ‘security principle,’ also known as the ‘integrity and confidentiality’ principle. Many digital media libraries use secure HTTPS communication with end-to-end TLS encryption, a function that encodes data in such a way that only authorised users can access it.

TLS security has 3 key attributes:

- **Authentication:** The server you are talking to is really the one you intended to
- **Confidentiality:** No-one else can read the data you send/receive
- **Integrity:** The data you receive has not been tampered with enroute

It’s a way of safeguarding against unauthorised or unlawful processing of personal data and enables you to demonstrate compliance with the security principle.



Having selected images for marketing materials, being able to provide quick, secure access to external suppliers is enormously helpful. The ability to add multiple tags and references makes the best use of the search functions and the dynamic folders mean that some are automatically updated as new images are uploaded - this has proven to be hugely time saving.”

Sarah Gowans, Marketing Manager at Bishop’s Stortford College

PERMISSIONS, CONSENT AND RECORD-KEEPING

Digital media libraries have several features that will help with permissions, consent and record-keeping, which are key aspects of data protection and privacy.



Site terms and conditions

When a user logs into their digital media library, you can require that they accept a set of terms and conditions. To avoid becoming a nuisance, once a user accepts the terms, this decision is recorded. In the case of Chorus digital media library for example, if you change your terms and need users to review them again, then there is a button to clear all existing terms and force users to go through this process again.

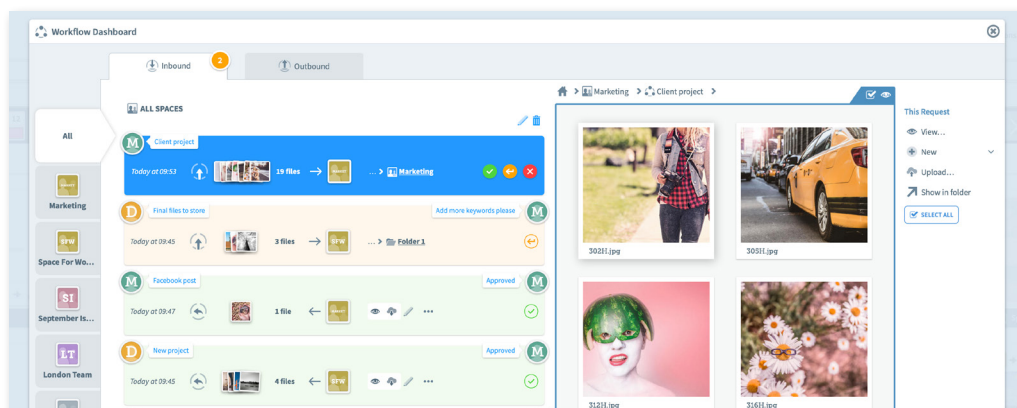
Many media libraries offer the ability to set a log retention policy, so that personal data is not stored indefinitely – GDPR specifically states you must not hold data for longer than is necessary.



Approvals and terms and conditions on key actions

Some digital media libraries include features which help you create manual approval workflows. For example, you can require that another user reviews their files at the stage of upload, so a team manager or a legal review department can check that all inbound files have been checked for copyright claims, restricted use or consent.

Similarly, you can use approvals on shares or downloads. This can be used to ensure that users consider any privacy implications before they re-use or publish a file, perhaps by drawing attention to your GDPR policies and ensuring that no inadvertent errors are made.

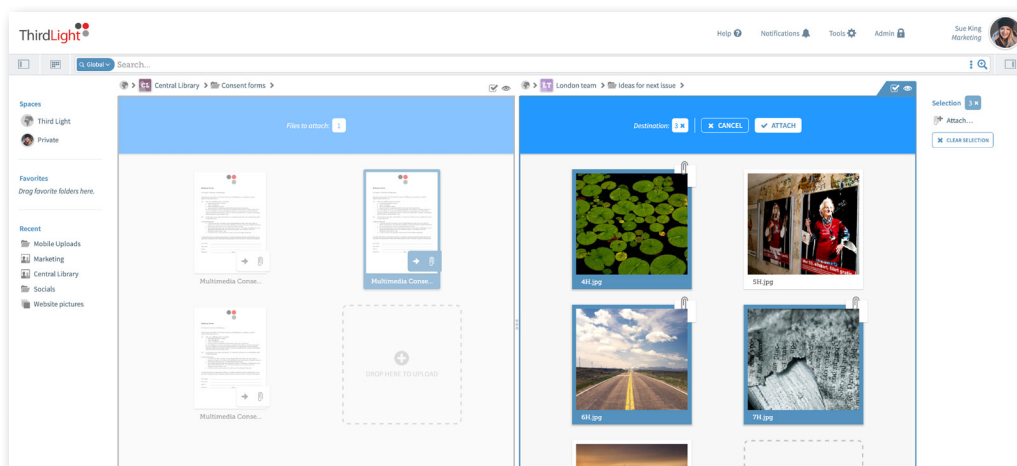


Attaching consent forms

When photography containing individuals is stored in your site, for example photos taken at an event, you may need to obtain consent from the person(s) depicted. This is generally achieved using a consent form which they sign, giving you the right to store the image. For your convenience, many digital media libraries enable you to attach consent forms to your actual files. This helps keep images and the relevant records for those images associated, assuming the consent form is a file. You can also add metadata to consents, like expiry dates, event related or name of the person so that it is easily searchable.

“As we are often taking shots of students on campus, having correct usage rights and consents is essential if we are providing the images as stock assets available to staff.”

Nathan Stewart, Production Manager, Image Services from Victoria University in New Zealand



Using metadata to record consent

Media libraries are built for metadata flexibility. For example, you can add custom metadata fields which can be drop-downs, yes/no options, tree structures or free text. If your media library offers a GDPR compliance package, you can use it for example to record consent, to maintain a log or to refer to other systems. Metadata fields can be protected from editing, again helping to stop information from being changed by accident or revealed in the wrong contexts.

Using metadata to recall records

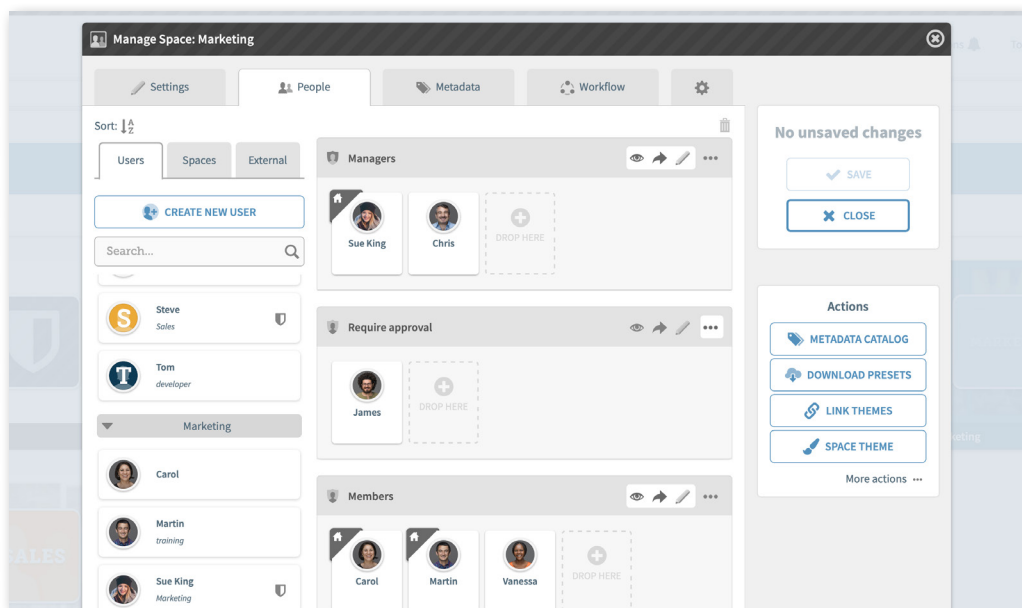
As part of the GDPR, individuals have a right to access their personal data, and when they do, metadata can be used to instantly recall specific records when data owners

or ‘subjects’ request them. Individuals also have the right to have personal data erased, known as ‘the right to be forgotten.’ Being able to recall all files with the same metadata from one centralised source can make erasing data quick and ensure accuracy.



Protected content

To make sure content and its associated personal data is well and truly secure and protected, a digital media library may allow you to set site, folder, user role and other organisational permissions. Using a unique security system, emailed links to published content can also be locked to individuals to prevent re-sharing – but without the need for a password to sign-in. Links to published content can also be embargoed or expired, watermarked and protected from forwarding to other users.



KEEPING COMPLIANT

With the rapid growth of the digital economy and huge increases in the volume of exchanges of personal data, manual processes simply can't keep pace with the expectations and obligations set out by current legislation. The collection of information about users and their habits and preferences, and automated decision-making both in public and private sectors, is rising at a dramatic rate, and consumers fear how their data is being used. Businesses must keep pace, or be faced with serious consequences and fines, so will inevitably have to invest in technology to help them do this. There's no doubt that implementing a good digital media library will enable businesses to meet many data protection requirements and is a clear step towards compliance with data privacy and in particular GDPR.

About Third Light

Third Light is a global software company based in Cambridge, UK. Our next-generation digital media library, Chorus, simplifies the storage and management of digital media files, or ‘digital assets’ and is accessible from anywhere and on any device. Powerful, robust and secure, it empowers marketing and content professionals to build a searchable library where they can collaborate and share digital media more efficiently.



Excellent   Trustpilot



01223 475674



thirdlight.com



ask@thirdlight.com



7330 Cambridge Research Park,
Waterbeach, Cambridgeshire, CB25 9TN



[@3rdlight](https://twitter.com/3rdlight)



linkedin.com/company/third-light-ltd



thirdlight.tv