GDPR

Compliance Guide

TABLE OF CONTENTS

CONTENTS

WHAT IS GDPR?

The EU General Data Protection Regulation ("GDPR") is a new comprehensive data protection law that updates existing EU laws to strengthen the protection of "personal data" (any information relating to an identified or identifiable natural person, so called "data subjects") in light of rapid technological developments, the increasingly global nature of business and more complex international flows of personal data. It replaces the current patchwork of national data protection laws with a single set of rules, directly enforceable in each EU member state. The GDPR took effect on May 25, 2018.

GDPR FAQ

Is there a GDPR certification?

No, there is not currently a GDPR certification issued by the European Commission. Eviid will be monitoring any certifications that come out after the GDPR goes into effect and will certify to them, if it deems them to be appropriate.

What is the difference between the “right to restrict processing” and the “consent management?

The right to restrict processing refers to the right of Data Subjects to request that a data controller block or suppress the processing of their personal data. Regarding consent management, in order to process personal data, organizations must have a lawful basis to process the data.
Under the GDPR, there are six legal bases which organizations can rely on to lawfully process personal data. One basis for processing is with the consent of the data subject. If an organization is relying on consent, and an individual requests a restriction of processing of their personal data, depending on the circumstance of the request, organizations may also want to consider whether to update the individual’s consent preferences to reflect their desire for personal data processing to cease. Organizations should seek legal counsel to understand what legal bases they are relying on to lawfully process personal data, their obligations under the GDPR, and then design their process.

How should we notify customer of these new rights?

The European Commission has a website with guidance for its citizens on GDPR.

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

GDPR FAQ

Does processing European personal data require the consent of the data subject?

Consent is only one of the legal bases one can use for the processing of personal data (Article 6(1)(a)). For instance, personal data can also be processed:

- when necessary for the performance of a contract to which the data subject (the individual whose data is processed) is a party;
- when there is a legal obligation to do so (such as the submission of employee data to a tax authority); and
- sometimes even on the basis of legitimate interests, such as commercial and marketing goals. The legitimate interest must, however, outweigh any detriment to the privacy of the data subject.

Do EU data subjects have an absolute right to have their personal data deleted upon request?

The right to have one's data deleted is often referred to as "the right to be forgotten". However, the right to be forgotten is not an absolute right. It has a limited scope and is subject to certain limitations (Article 17). In most cases, when considering a request for deletion several relevant factors have to be taken into account; this right will not apply, for example, if the processing is necessary for compliance with a legal obligation.
However, data subjects do have an absolute right to prevent their personal data from being processed for direct marketing purposes.

EVIID AND GDPR

What does eviid collect by default?

By default eviid collects location data which it embeds within the media and links to a client generated Unique Reference number, for example a claim ID or job reference number, for the purpose of evidence that a piece of media was collected in a particular place at a particular time. At this point, the data is effectively anonymous as there isn't any personal data associated with the media.

It is up to the client what additional data is to be added to the media or collected using questionnaires. This can be anything from simple Surname and Post Code data to complex data around a particular scenario.

What is the retention period of the data?

Our clients can specify the data retention period as part of their contract. This is a configuration item within the eviid portal after which time the data is automatically and permanently deleted from the system. Where not specified, the default retention period is 7 years, as the data could be used to support or reject a financial claim, the records for which would need to be retained for that period.

Does eviid encrypt items at rest?

We do encrypt items at rest. It is worth noting however that the GDPR does not mandate specific security measures. Instead, the GDPR requires organizations to take technical and organizational security measures which are appropriate to the risks presented (Article 32(1)). Encryption at rest and pseudonymization may be appropriate depending on the circumstances, but they are not mandated by the GDPR in every instance.

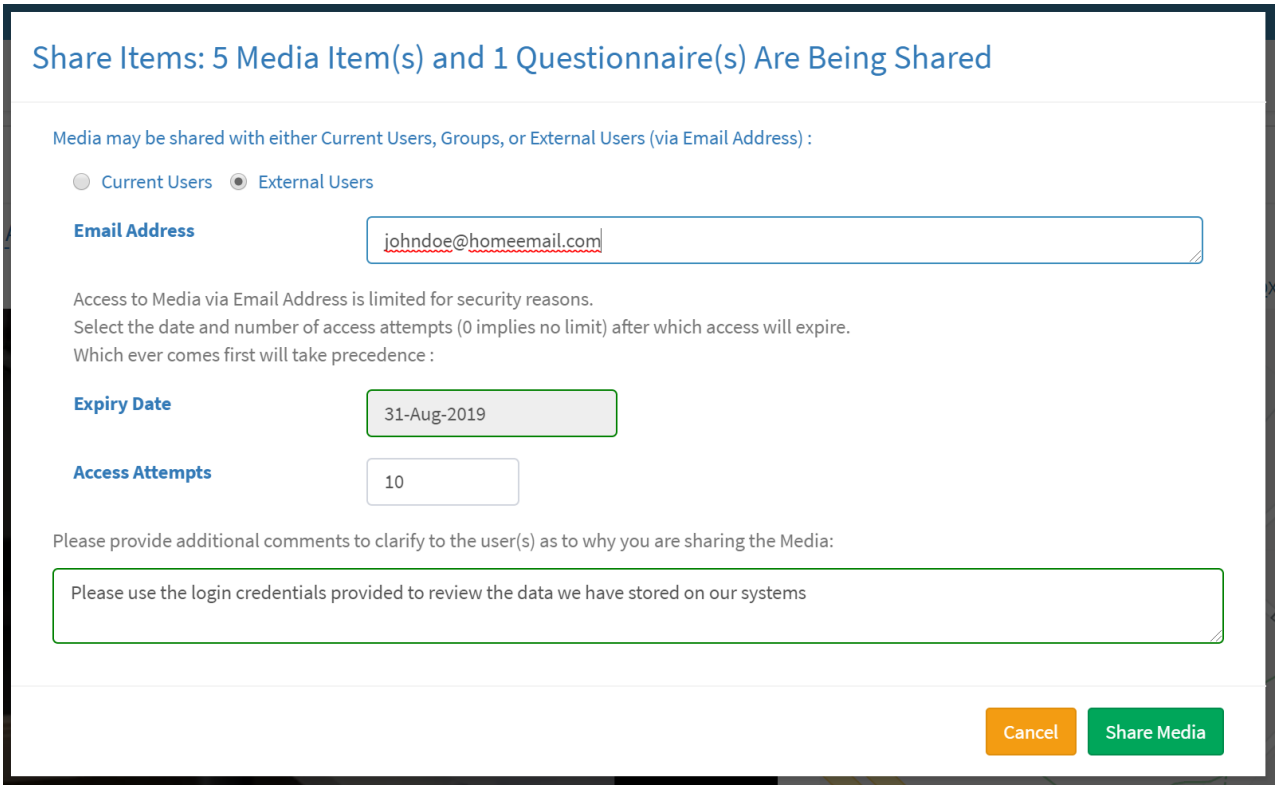
EVIID AND GDPR

How does eviid deal with consent?

It is up to the client to design into their processes getting customer consent to collect their data. However, eviid can accomodate this in a number of different ways, the most common being to have a Customer Consent form available in the professional app to capture a customer's signature when a field agent visits a customer's premises, and having an appropriate Ts & Cs window appear on opening client's business to consumer applications which requires the customer to consent to it's use while guiding them to the clients privacy guidelines which are typically held on the client's website.

How does eviid deal with 'information requests'?

Our clients can very swiftly respond to a customer's request to view data held on them using the audited sharing capability of the system. Where a request is made to eviid directly, we will contact the assigned client liaison to ensure the request is actioned within the regulated timeframe.

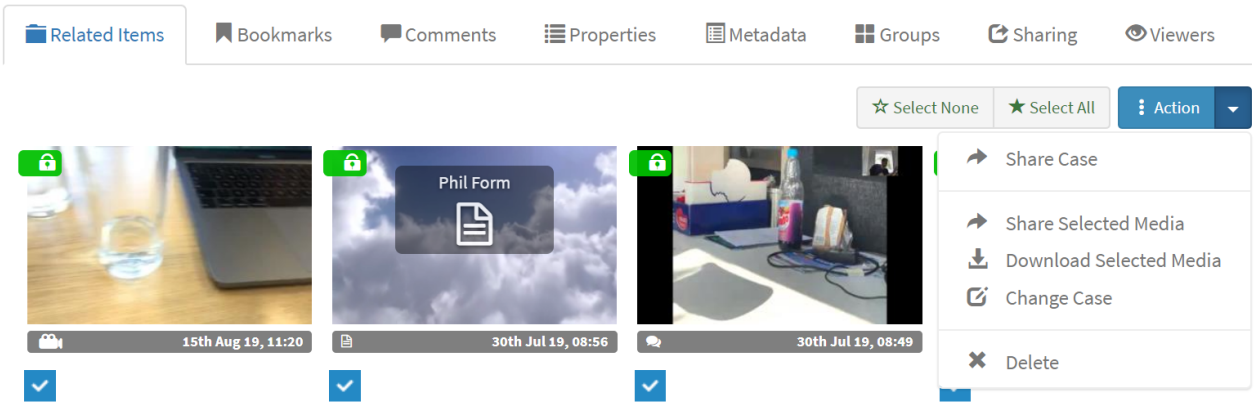


EVIID AND GDPR

How does eviid deal with 'right to be forgotten'?

Clients whose Data Subjects request their information is removed can accommodate this through their site administrator(s) who can select the data items and chose delete from the actions menu.

All actions in the portal are audited so the who and when of this action is stored for future reference. The data items themselves are soft deleted until the end of the retention period but are completely inaccessible to the client in line with the FAQ earlier in this document. However, a further hard delete option is available should future GDPR regulation make this an absolute requirement.



FURTHER INFORMATION

Who do I contact should I have further questions?

We are happy to answer any further questions you may have.
You may contact us by phone on 0333 800 388 or email at support@eviid.com
or write to
Data Protection Officer, Eviid, 520 Birchwood Boulevard, Warrington, Cheshire. WA3 7QX