Privacy notice for audits of slaughterhouses and GHEs

Information on our privacy notice for audits of slaughterhouses and game handling establishments (GHEs) setting out what information we collect, what we do with the data and your rights.

The FSA has a statutory duty to audit slaughterhouses and GHEs in England and Wales in accordance with requirements of Official Controls. Audit Inspections involve a tour of the premises, observation of practices, inspection of product, condition of animals and a review of procedures and records. The FSA conducts such audit inspections either through a site visit or remotely using a software application which enables FBO staff ('the business representative') on site to livestream footage to The Veterinary Auditor ('the auditor').

What information we will collect

The audit information will be collected by the Official Veterinarian (OV) with the assistance of the business representatives. Audit inspections involve assessing premises and processes by sight, whether on premise or remotely, and obtaining copies of process documentation, taking photographs and recording footage relevant to the audit at the time of the visit.

The auditor therefore will make observations about business premises and processes and only capture and retain information where it is relevant audit evidence.

A remote audit uses a software application which allows the business representative to livestream footage from the site to the auditor who will only see what they are shown and will follow strict processes when undertaking the audit. The application also allows the auditor to capture images or recording footage from the livestream. The auditor will make it clear when they are taking images or recording footage. The application will also indicate to the business representative when the auditor is viewing, recording and capturing images.

As well as business information, the audit process may also capture a limited amount of personal information such as the email and contact details of business representatives assisting the auditor with the audit, and incidental information that may form part of any audit evidence.

In addition when the audit takes place using the remote audit software, the software may log data including login credentials, user names, user email addresses, IP addresses, geographic locations and device IDs.

Legal basis

The FSA needs to collect this information in the exercise of the official authority vested in it, to carry out Official Controls, and in the performance of its Public Task which is carried out in the public interest.

What we do with it

The auditor will review information collected as audit evidence to compile the audit report. Any information that is required to be retained to support audit findings and observations is stored and linked to the final report.

Information provided will also be used to arrange the audit whether it be a site visit or to facilitate the business in setting up the remote audit applications. Where guest licences to the remote audit software are provided those licences will expire after the audit. Guidance will be provided on the use of the application. For remote audits the application collects call log details described to administer the connection between the business and the auditor to facilitate the livestreaming of the audit.

All the information and data collected by the auditor for audit purposes is captured, stored and used in accordance with official guidance in the Manual of Official Controls and in accordance with FSA policies and guidelines.

How and where we store your data and who we may share it with

Audit evidence held in FSA systems is stored in accordance with the Government Security Policy Framework, Government Minimum Security Cyber Standard and National Cyber Security Cloud Principles. We treat the security of your information very seriously and only process it in accordance with our Information Security Standards and Policies. All personnel involved in the audit process are trained to manage information collected through audits responsibly and securely. Personal information is not captured unless it is relevant and necessary.

For financial, organisational or technical reasons, we may engage third parties to process data on our behalf. Where we conduct remote audits we will use Librestream Onsight Applications and cloud based servers to facilitate the livestream call and the capture of images and recorded footage. More information can be found on Librestream's Security and GDPR compliance statement.

We will not share your information with any such third party unless we are satisfied that they are able to provide an adequate level of protection in respect of your information. We do this by taking steps to ensure that these organisations have in place suitable technical and organisational safeguards either through contracts or agreements we hold with them and/or by obtaining robust assurances from them that they operate in accordance with the UK GDPR. Where we have a legal basis to send or transfer personal data to third parties based in countries outside the UK we will ensure appropriate safeguards are in place in accordance with UK GDPR. No other third parties have access to your personal data unless the law allows them to do so.

Retention

The auditors are committed to delete the information gathered during the remote audit process within 10 days of submission of the audit report (with exception of evidence that need to be kept for enforcement purposes) as agreed in previous meetings with Industry. To verify compliance with this, random spot checks will be carried out to assure compliance with the policies and guidelines.

Your rights

You have a right to see the information we hold on you by making a request in writing to the email address below. If at any point you believe the information we process on you is incorrect you can request to have it corrected. If you wish to object to the processing of your personal data or raise

a complaint on how we have handled your data, you can contact our Data Protection Officer who will investigate the matter.

If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law you can complain to the Information Commissioner's Office (ICO).

Contact us

Our Data Protection Officer in the FSA is the Information Management and Security Team Leader who can be contacted at the email address informationmanagement@food.gov.uk